EXHIBIT A

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**TO BE FILED UNDER SEAL**
	:	
v.	:	Hon. Leda Dunn Wettre
	:	
ALLEN GILTMAN	:	Mag. No. **20-13462**
	:	
	:	**CRIMINAL COMPLAINT**

I, Andrew Feiter, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Andrew Feiter

Andrew Feiter, Special Agent
Federal Bureau of Investigation

Special Agent Feiter attested
to this Complaint by telephone
pursuant to FRCP 4.1(b)(2)(A) on
October 26, 2020 in the
District of New Jersey

HONORABLE LEDA DUNN WETTRE
UNITED STATES MAGISTRATE JUDGE

Leda Dunn Wettre

Signature of Judicial Officer

ATTACHMENT A

COUNT ONE

(Conspiracy to Commit Wire Fraud)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

did knowingly and intentionally conspire with others to devise and intend to devise a scheme and artifice to defraud individuals, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Sections 1349 and 2.

COUNT TWO

(Conspiracy to Commit Securities Fraud)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

knowingly and intentionally conspired and agreed with others to, by use of the means and instrumentalities of interstate commerce, the mails, and facilities of national securities exchanges, directly and indirectly, knowingly and willfully use manipulative and deceptive devices and contrivances in contravention of Title 17, Code of Federal Regulations, Section 240.10b-5 in connection with the purchases and sales of securities, to wit, Certificates of Deposit offered through various fictitious entities, by (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, namely, persons with interests in the fictitious Certificates of Deposit, contrary to Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

In violation of Title 18, United States Code, Section 371.

COUNTS THREE AND FOUR

(Aggravated Identity Theft)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, described in the table below, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another actual person, each constituting a separate count of this Complaint:

Count	Approximate Date	Initials of Identity Theft Victim	Means of Identification
3	April 4, 2019	M.K.	Name CRD Number
4	July 31, 2019	P.S.	Name CRD Number

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

ATTACHMENT B

I, Andrew Feiter, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed since November 2019. I am currently assigned to the Newark, New Jersey Field Office. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

2. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a federal criminal complaint and arrest warrant, I have not included each and every fact known by the Government concerning this investigation. Except as otherwise indicated, the actions, conversations, and statements of others identified in this Affidavit – even where they appear in quotations – are reported in substance and in part. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided.

PROBABLE CAUSE

I. Overview of the CD Fraud Scheme

3. The FBI is investigating an ongoing computer and wire fraud scheme that there is probable cause to believe is being executed by Allen GILTMAN ("GILTMAN") and others (the "Subjects"). In furtherance of the scheme, the Subjects have created fraudulent websites (the "Fraud Websites") to solicit funds on the internet from individuals seeking to invest money. At times, the Fraud Websites were designed to closely resemble websites being operated by actual, well-known, and publicly reputable financial institutions. For instance, the Fraud Websites "www.bnymelloncdrates.com" and "www.bnymellonpershing.com" were created to appear as real websites that were operated by and promoting the sale of investment products by the Bank of New York, an actual, well-known, and publicly reputable financial institution. At other times, the Fraud Websites were designed to resemble legitimate-seeming financial institutions that did not, in fact, exist. For example, the Fraud Websites "www.marlowefinancial.com," and "www.marlowfinancial.com" each purported to offer the investment services of a fake company calling itself "Marlow Financial."

4. The Subjects used a variety of means to make the Fraud Websites

appear legitimate and to gain and maintain the trust of prospective investors, including by:

a. displaying the actual names and logos of real financial institutions;

b. purporting that the institutions were members of and/or regulated by the Federal Deposit Insurance Corporation ("FDIC"), Financial Industry Regulatory Authority ("FINRA"), the Securities Investor Protection Corporation ("SIPC"), or New York Stock Exchange;

c. claiming that deposits made to the institutions associated with the Fraud Websites were FDIC insured; and

d. using FINRA and/or FDIC member identification numbers issued to real financial institutions and broker-dealers.

5. The Fraud Websites advertised various types of investment opportunities, most prominently the purchase of certificates of deposit ("CDs"). The Fraud Websites advertised higher than average rates of return on the CDs, which enhanced the attractiveness of the investment opportunities to potential victims.

6. Victims of the fraud, which is described herein as the "CD Fraud Scheme," typically discovered the Fraud Websites via internet searches. In furtherance of the scheme, the Subjects purchased internet advertising, which caused advertisements for the Fraud Websites to appear in Google and Microsoft Bing search results for searches including phrases such as "best CD rates" or "highest cd rates." As a result, unsuspecting investors, when conducting such internet searches, received advertisements for the Fraud Websites on their web browsers and clicked on links that directed them to the Fraud Websites.

7. Multiple victims of the CD Fraud Scheme attempted to purchase CDs that were offered through one or more of the Fraud Websites. In many instances, the victim would contact an individual via telephone or email as directed on a Fraud Website (the "Fraud Contact"). As set forth herein, there is probable cause to believe that, in many instances, the Fraud Contact was, in fact, GILTMAN, purporting to be someone else.

8. In multiple instances involving Fraud Websites that spoofed websites maintained by actual financial institutions, the Fraud Contact impersonated an actual employee of the financial institution whose name and imagery were depicted on the Fraud Website and used the real employee's name and FINRA CRD number.[1]

[1] FINRA operates the Central Registration Depository ("CRD"), the central licensing and registration system used by the U.S. securities industry and its

9. The Fraud Contact ultimately caused the victim to receive various documents, including, but not limited to, account applications, term sheets, and wiring instructions related to the purchase of a CD. The victim completed and submitted the paperwork, followed the wiring instructions, and wired funds to the bank account specified by the Fraud Contact. The funds then were moved out of the specified bank account to various international and domestic bank accounts.

10. Law enforcement has determined that the funds transmitted by the victims in accordance with the above-described procedure were not used to procure CDs or any other advertised investment products, and none of the victims actually took ownership of the products that they intended to purchase.

11. The Subjects have gone to significant lengths to hide their true identities and to perpetuate the CD Fraud Scheme. For example, they have used: (a) virtual private networks ("VPNs") to anonymize their digital footprints, such as IP addresses; (b) prepaid gift cards to pay for domain-name registration services, state incorporation filings, internet ads, and VPN, website, and call-answering services; (c) prepaid phones or encrypted communication products to communicate with victims of the CD Fraud Scheme; and (d) fake invoices and websites to explain large money transfers in response to inquiries by banks that received large wire transfers of investor funds.

12. To date, the investigation has identified at least 70 victims of the CD Fraud Scheme, who collectively transmitted funds that they believed to be investments in the amount of at least approximately $50 million. Law enforcement has further identified at least approximately 130 Fraud Websites operated by the Subjects as part of the CD Fraud Scheme. The most recent Fraud Website identified by law enforcement as part of the CD Fraud Scheme was registered on or about October 16, 2020.

II. Individuals, Entities and Bank Accounts

13. At various times relevant to this Complaint:

a. GILTMAN was a resident of California.

b. GILTMAN was the registered agent of Irelle Financial Corporation ("Irelle"), a California company, and maintained a bank account under the name "Irelle Corporation" at Wells Fargo Bank.

c. Victims -1, -4, and -10 were residents of Texas.

d. Victims -2 and-3 were residents of Connecticut.

---

regulators, which contains the registration records of broker-dealer firms and their associated individuals (*e.g.*, brokers and investment advisors).

e. Victims -5, and -12 were residents of Florida.

f. Victims -6 and -11 were residents of New Jersey.

g. Victim-7 was a resident of Massachusetts.

h. Victims -8 and -9 were residents of Georgia.

i. Victim-13 was a resident of Illinois.

j. Victim-14 was a resident of New York.

k. Individual-1 was a resident of Pennsylvania.

l. R.H., R.P., P.S., M.K., A.F., and R.W. were broker-dealers registered with FINRA.

III. The AT&T Prepaid Phones

14. Through this investigation, law enforcement has identified several AT&T prepaid phone numbers used by the Subjects in furtherance of the CD Fraud Scheme, including numbers ending in 6712 (the "6712 Number"), 1728 (the "1728 Number"), 3703 (the "3703 Number"), 2574 (the "2574 Number"), and 0968 (the "0968 Number") (collectively, the "AT&T Prepaid Phones"). The AT&T Prepaid Phones have been used by the Subjects to, for example: (a) register Fraud Websites with web-hosting providers; (b) communicate with numbers listed on the Fraud Websites to make sure the numbers were working properly; and (c) speak with victims of the CD Fraud Scheme, as set forth in the paragraphs below.

A. *The 6712 Number*

1. *Victim-1*

15. In or around October 2017, Victim-1 conducted an internet search for CDs and discovered the Fraud Website "www.marlowefinancial.com." Victim-1 called a phone number listed on the website and spoke to a Fraud Contact, who used the name of a real broker-dealer registered with FINRA with the initials R.H. (the "R.H. Fraud Contact"). The R.H. Fraud Contact told Victim-1 that "Marlowe Financial" brokered CDs from banks such as Citibank and Bank of America.

16. On or about October 20, 2017, the R.H. Fraud Contact sent Victim-1 an introductory email, which included an application for a CD, a fictitious CD term sheet, and an example of FDIC coverage. In the introductory email, the R.H. Fraud Contact again used the name of R.H. and a CRD number belonging to R.H. without R.H.'s authorization. Victim-1 thereafter applied for three CDs totaling approximately $1 million.

17. On or about October 24, 2017, the R.H. Fraud Contact sent Victim-1 an email with wiring instructions, which directed Victim-1 to wire funds to an account at TBC Bank in Tbilisi, Georgia held by an entity called "Principal Financial Limited" (the "TBC Bank Account"). Victim-1 wired the funds as instructed. In the email, the Fraud Contact provided Victim-1 with a "direct phone" number ending in 5681 (the "5681 Number").

18. On or about October 30, 2017, the Fraud Contact sent Victim-1 an email with fictitious statements related to the CDs "purchased" by Victim-1, which falsely depicted "interest earned" on the CDs as of the date of the email.

19. In or around December 2017, Victim-1 emailed the Fraud Contact to request original documents associated with the CDs that Victim-1 believed he/she had purchased. The Fraud Contact responded that the documents would be delivered to Victim-1's home by December 18, 2019.

20. On or about December 19, 2017, after not receiving the promised documents, Victim-1 twice attempted to call the Fraud Contact. According to phone records, these phone calls connected to the 6712 Number and went to voicemail. Thereafter, Victim-1 was unable to reach the Fraud Contact and never received a CD or any other investment product related to the transfer of funds described above.

2. *Victims-2 and -3*

21. In or around January 2018, Victim-2 conducted an internet search related to CDs and discovered the Fraud Website "www.principalfinancialgroupllc.com," which offered investment services through a fictitious entity called "Principal Financial Group." Victim-2 called a number listed on the Fraud Website and spoke with an individual using the name of a real broker-dealer registered with FINRA with the initials R.P. (the "R.P. Fraud Contact"). The R.P. Fraud Contact provided Victim-2 with information about FDIC limits associated with a CD promoted on the Fraud Website.

22. Victim-2's spouse, Victim-3, thereafter exchanged several emails with the R.P. Fraud Contact regarding the purchase of an FDIC insured "84 Month Jumbo CD." On or about January 18, 2018, Victim-3 received an email from the R.P. Fraud Contact welcoming Victim-2 and-3 as customers of "Principal Financial." The R.P. Fraud Contact, claiming to be a "Sr. Account Executive" with Principal Financial Group, again used the name of R.P. without R.P.'s authorization and provided the 5681 Number as a "direct phone" number - the same number provided by the R.H. Fraud Contact to Victim-1. The email further provided a fictitious account number for the CD and wiring instructions, which directed Victims-2 and -3 to wire funds to the TBC Bank Account. Victims-2 and -3 wired funds totaling approximately $242,300, as instructed, on the same date.

23. On or about January 19, 2018, Victims-2 and -3 attempted to call the R.P. Fraud Contact regarding their CD. This phone call connected to the 6712 Number and went to voicemail. Victims-2 and -3 were unable to reach the R.P. Fraud Contact and never received a CD or any other investment product related to the transfer of funds described above.

3. *Additional Information*

24. Between January 4, 2018, and February 2, 2018, the 6712 Number called the number 1-866-570-9585 on four occasions, which, during this time period, was the phone number listed on several Fraud Websites associated with the CD Fraud Scheme, including "www.theprincipalgroupllc.com," "www.marlowfinance.com," and "www.marlowecdrates.com."

25. Further, the investigation revealed that the 6712 Number was listed as the phone number for a Google email address that referenced R.H.'s name (the "R.H. Google Email Account"), but that R.H. did not create, control, or authorize. The R.H. Google Email Account was used to register at least one Fraud Website, "www.principalbrokerage.com," and was listed as a secondary email account for the Fraud Website "www.principalfinancialgroupllc.com" – the Fraud Website visited by Victims-2 and -3.

B. *The 3703 Number*

1. *Victim-4*

26. In or around November 2018, Victim-4 discovered the Fraud Website "www.federaluniversal.com," which purported to offer the investment services of an entity called "Universal Community Federal Savings Bank." Victim-4 called a number listed on the Fraud Website and spoke with an individual using the name of a real broker-dealer registered with FINRA with the initials M.K. (the "M.K. Fraud Contact"). According to Victim-4, the M.K. Fraud Contact told Victim-4 that he was located in the "financial district of Los Angeles."

27. On or about November 9, 2018, Victim-4 received an introductory email from the M.K. Fraud Contact, which included an application for a CD. The email stated, "Universal Bank is a full service, global financial institution," and represented that its products were FDIC insured. In the introductory email, the M.K. Fraud Contact again used M.K.'s name and a CRD number belonging to M.K. without M.K.'s authorization. Victim-4 thereafter applied for three CDs totaling approximately $500,000.

28. On or about November 12, 2018, Victim-4 received an email welcoming him/her as a customer and stating that his/her account was "active" and "ready for funding." The email further provided wiring instructions, which directed Victim-4 to wire funds to a bank account in Poland (the "Poland Bank Account"). Victim-4 wired the funds as instructed.

29. According to Victim-4, after he/she wired an initial $500,000, he/she received a call from the M.K. Fraud Contact, who stated that the bank was currently offering a "special" on CDs with an attractive, lower interest rate. After speaking to the M.K. Fraud Contact, Victim-4 wired an additional $500,000 to the Poland Bank Account per the M.K. Fraud Contact's instructions. Victim-4 never received a CD or any other investment product related to the transfer of funds described herein.

30. According to phone records, Victim-4 received a phone call from the 3703 Number on or about November 30, 2018, consistent with Victim-4's statement.

2. *Victim-5*

31. In or around January 2019, Victim-5 discovered the Fraud Website "www.federaluniversal.com," the same Fraud Website visited by Victim-4, which now purported to offer the financial services of a different entity called "Broadway Financial Group." The Frau Website again listed M.K.'s name and the same email address used by the M.K. Fraud Contact when communicating with Victim-4. After being provided with a CD application via email, Victim-5 opted to purchase a CD in the amount of approximately $185,000.

32. On or about January 30, 2019, Victim-5 received an email from the M.K. Fraud Contact, who again used M.K.'s name and CRD number without M.K.'s authorization. The email stated that Victim-5's account was "active" and "ready for funding" and provided wiring instructions similar to those provided to the victims referenced previously, which directed Victim-5 to wire funds to an account he/she believed belonged to "Broadway Financial Group." Victim-5 wired the funds as instructed.

33. On or about January 31, 2019, Victim-5 received an email from the M.K. Fraud Contact acknowledging the receipt of Victim-5's funds. According to Victim-5, the email listed an incorrect amount associated with the purchase of Victim-5's CD. Victim-5 became suspicious regarding the error and traveled to his/her bank to inquire about the status of the wire he/she sent. Victim-5 was informed by bank officials that the funds he/she wired were not sent to an account held by "Broadway Financial Group" as Victim-5 believed, but were rather sent to an account held at HSBC Bank by an entity called "HRC Global, LLC" (the "HRC Bank Account"). The funds were then wired to another bank account located in Hong Kong.

34. The next day, on or about February 1, 2019, Victim-5 placed at least six calls to the Fraud Contact to discuss his/her CD. Each of these calls, including one lasting approximately 2 minutes and 13 seconds, connected to the 3703 Number. To date, Victim-5 has not received a CD or any other investment product related to the transfer of funds described above.

3. *Additional Information*

35. On or about August 24, 2018, the 3703 Number called a number for TransferWise. TransferWise is an international money transfer service that at least one victim of the CD Fraud Scheme used to transfer money on the belief that he/she was purchasing a CD.

36. On or about November 15, 2018, the 3703 Number called the phone number 1-866-740-5001, which, at the time, was the phone number listed on the Fraud Website "www.midwestbankgroup.com."

37. In or around April 2019, another victim of the CD Fraud Scheme, Victim-6, visited the Fraud Website "www.midwestbankgroup.com," and wired approximately $200,000 for the purchase of a CD that Victim-6 never received. Similar to Victims -4 and -5, Victim-6 also communicated with the M.K. Fraud Contact, including an email sent to Victim-6 on or about April 4, 2019, in which the M.K. Fraud Contact used the name and CRD number of M.K. and provided Victim-6 with an application for a CD.

C. *The 2574 Number and 1728 Number*

1. *Victim-7*

38. In or around June 2019, Victim-7 discovered the Fraud Website "www.globalbankinggroupfsa.com," which purported to offer the investment services of an entity called "Global Banking Group."

39. On or about June 26, 2019, Victim-7 received an email from a Fraud Contact who used the name and CRD Number of a real broker-dealer registered with FINRA with the initials "P.S." (the "P.S. Fraud Contact"). The P.S. Fraud Contact claimed to be a "Senior Account Executive" with "Global Banking Group." The email further claimed, similar to emails received by the previous victims, that Global Bank was a "registered FDIC Institution" that offered "securities" through various FINRA/SIPC member banks such as Citibank and JP Morgan Chase. The email included an application for a "15 Month Jumbo CD."

40. On or about June 27, 2019, after completing the application provided by the P.S. Fraud Contact, Victim-7 received an email informing him/her that his/her account was "active" and "ready for funding." The email provided an account number associated with a $500,000 CD and listed a "direct phone" number for the Fraud Contact ending in 9616 (the "9616 Number"). The email further provided wiring instructions, which directed Victim-7 to wire the funds to an account held at Citibank by an entity called "HDF Global, LLC" (the "HDF Bank Account"). Victim-7 wired the funds as instructed.

41. On or about July 11, 2019, Victim-7 called the P.S. Fraud Contact regarding his/her CD. This phone call connected to the 2574 Number and lasted for approximately five minutes and seven seconds. The length of this

phone call suggests that Victim-7 and the P.S. Fraud Contact spoke about the CD that Victim-7 believed he/she had purchased and that Victim-7's call did not simply go to voicemail. Victim-7 never received a CD or any other investment product related to the transfer of funds described herein.

2. *Victims-8 and -9*

42. In or around June 2019, married couple Victims-8 and -9 discovered the Fraud Website "www.globalbankinggroupfsa.com," the same Fraud Website visited by Victim-7, after conducting an internet search for "high CD return banks." The Fraud Website advertised the services of an entity called "Global Banking Group." Similar to Victim-7, Victims-8 and -9 also communicated by phone and email with the P.S. Fraud Contact, who also provided Victims-8 and -9 with the 9616 Number.

43. On or about June 28, 2019, Victims-8 and -9 wired approximately $750,000 to the HDF Bank Account per instructions provided by the P.S. Fraud Contact. Approximately one week later, the Fraud Contact emailed Victims-8 and -9 and provided a fictitious statement regarding the status of Victims-8 and -9's CD and interest accrued on the CD to date.

44. Victims-8 and -9 became suspicious after not receiving any additional account statements. On or about July 11, 2019, Victims-8 and -9 called the P.S. Fraud Contact to inquire about the status of their CD. According to AT&T records, the call connected to the 2574 Number and lasted approximately three minutes. According to Victims-8 and -9, the P.S. Fraud Contact advised them to "give it another week" before calling back.

45. On or about July 9, 2019 the 2574 Number called the 1728 Number – the same day that the prepaid account associated with the 1728 Number was activated. Based on information learned during this investigation, the Subjects would often use one AT&T Prepaid Phone to call another, particularly when a new AT&T Prepaid Phone was first activated. Similarly, AT&T records show that the 2574 Number and the 1728 Number frequently called, or were called by, the 9616 Number, with the majority of the calls lasting just seconds. Based on this investigation, there is probable cause to believe that the Subjects were engaging in this practice in order to "test out" the AT&T Prepaid Phones, and other phones used by the Subjects, throughout the course of the CD Fraud Scheme.

46. On or about July 18, 2019, Victims-8 and -9 attempted to call the P.S. Fraud Contact approximately ten times to inquire about the status of their CD, but the calls went to voicemail. These calls all connected to the 1728 Number and lasted for just seconds each, consistent with the calls going to voicemail. Previously, as referenced above, calls made by Victims-8 and -9 to the Fraud Contact connected to the 2574 Number. Based on this information, there is probable cause to believe that the 9616 Number provided to Victims-8 and -9 by the Fraud Contact was forwarding to the 2574 and 1728 Numbers.

47. To date, Victims-8 and -9 have not received a CD or any other investment product related to the transfer of funds described above.

3. *Victim-10*

48. In or around July 2019, Victim-10 discovered the Fraud Website "www.westernalliancegroupfsa.com" after conducting an internet search for attractive CD rates. The Fraud Website purported to offer the financial services of a fictitious entity called "Western Alliance Banking Group."

49. On or about July 31, 2019, Victim-10 received an email from the P.S. Fraud Contact, the same Fraud Contact that communicated with Victims -7, -8, and -9 through various fictitious entities. The email provided Victim-10 with an application for a CD, which Victim-10 immediately completed.

50. On the same date, Victim-10 received another email from the P.S. Fraud Contact stating that his/her account was "active" and "ready for funding." The email further claimed, similar to the emails received by the victims described above, that "Western Alliance Bank is a Registered FDIC Institution" and that it offered "securities" through various financial institutions such as JP Morgan Chase, Citibank, and BB&T Bank. The email further provided wiring instructions, which directed Victim-10 to wire funds to an account held at BB&T Bank under the business name "HDS Global" (the "HDS Global Bank Account").

51. On or about August 1, 2019, Victim-10 wired approximately $250,000 to the HDS Global Bank Account per the P.S. Fraud Contact's instructions. Victim-10 thereafter received an email that confirmed receipt of the wire transfer and provided Victim-10 with a fictitious account statement showing an "opening balance" for his/her CD.

52. Victim-10 called the 1728 Number on or about August 8, 2019 and the call went to voicemail. Victim-10 never received a CD or any other investment product related to the transfer of funds described above.

4. *Additional Information*

53. On or about July 13, 2019, the Fraud Website "westernalliancebankgroup.com" was registered. Payment contact information associated with the account that created the site listed P.S.'s name and the 1728 Number.

54. On or about July 12, 2019, July 15, 2019, July 17, 2019, and July 18, 2019, the 1728 Number called numbers, which were, at the time, listed on the Fraud Websites "www.globalbankinggroupfsa.com," "www.calbusinessbank.com," "www.calcommercebanking.com," and "www.commerceonefsa.com," respectively.

55. In or around July 2019, another victim of the CD Fraud Scheme,

Victim-11, visited the Fraud Website "www.westernalliancebankgroup.com," and wired approximately $700,000 for the purchase of a CD that Victim-11 never received. Similar to Victims -7, -8, -9, and -10, Victim-11 also communicated with the P.S. Fraud Contact, including an email sent to Victim-11 on or about July 31, 2019, in which the P.S. Fraud Contact used the name and CRD number of P.S. and provided Victim-11 with an Application for a CD.

56. On or about August 19, 2019 the Fraud Website "visionbankingroup.com" was registered. The payment contact information for the account listed P.S.'s name and the 2574 Number.

D. *The 0968 Number*

1. *Victim-12*

57. In or around May 2020, Victim-12 conducted an internet search and discovered the Fraud Website "www.globalwealthhsbc.com," which purported to offer the investment services of an entity called "Global Financial Group – HSBC Wealth Management." According to Victim-12, he/she sent an email to an address displayed on the Fraud Website to inquire about purchasing a CD.

58. On or about May 12, 2020, Victim-12 received an email from a Fraud Contact who used the name and CRD number of a real broker-dealer registered with FINRA with the initials A.F. (the "A.F. Fraud Contact"). The email included an application for a CD similar to those received by previous victims of the CD Fraud Scheme.

59. On or about May 21, 2020, after returning a completed application form to the A.F. Fraud Contact, Victim-12 received an email stating this his/her account was "active" and "ready for funding." The email included wiring instructions, which directed Victim-12 to wire funds to a bank located in China. Shortly thereafter, Victim-12 wired approximately $500,000 per the Fraud Contact's instructions.

60. After completing the above transaction, Victim-12 continued to communicate with the Fraud Contact by email and phone and subsequently wired an additional $640,000 in two separate transactions for the purchase of two additional CDs through the fictitious Global Financial Group entity.

61. On or about June 18, 2020, after wiring additional funds as referenced above, Victim-12 emailed the A.F. Fraud Contact with the subject line "Call back" and stated, "I have been trying to reach you all day." The following day, on or about June 19, 2020, the Fraud Contact responded to Victim-12's email and stated, "I would like to give you my personal direct number," and listed the 0968 Number.

62. According to AT&T records, on or about June 18, 2018, the 0968 Number called Victim-12 and dialed *67 before making the call to mask the

number. The call lasted approximately three minutes and thirty-seven seconds. Further, Victim-12 called the 0968 Number at least five times between May 15, 2020 and May 20, 2020 leading up to Victim-12's initial investment through the Fraud Website. These calls occurred prior to the Fraud Contact's providing Victim-12 with the 0968 Number. There is therefore probable cause to believe that, similar to the other AT&T Prepaid Phones discussed previously, calls from victim investors were being forwarded to the 0968 Number from other numbers provided to the victims on the Fraud Websites or by a Fraud Contact through email.

63. To date, Victim-12 has not received a CD or any other investment product related to the transfer of funds described above.

2. *Victim-13*

64. In or around February 2020, Victim-13 conducted an internet search for "highest rate CD" and discovered the Fraud Website "www.synovuswealth.com," which purported to offer the investment service of an entity called "Synovus Wealth Group." Victim-13 communicated with a Fraud Contact using the name and CRD number of a real FINRA broker-dealer with the initials "R.W." (the "R.W. Fraud Contact").

65. On or about February 21, 2020, prior to purchasing a CD, Victim-13 called the 0968 Number and the call went to voicemail.

66. On or about February 24, 2020, Victim-13 received an email from the R.W. Fraud Contact. The email provided Victim-13 with an application for a CD and contained language that was nearly identical to the language in emails sent to previous victims of the CD Fraud Scheme.

67. On or about February 25, 2020, Victim-13 emailed a completed application for a CD to the R.W. Fraud Contact. The Fraud Contact responded by email, which indicated that Victim-13's account was "active" and "ready for funding." The email also included wiring instructions, which directed Victim-13 to wire funds to a Wells Fargo Bank account held under the business name AGQ Business Group LLC (the "AGQ Bank Account").

68. On February 25, 2020, Victim-13 wired approximately $232,000 to the AGQ Bank Account as instructed.

69. On February 26, 2020, the Fraud Contact emailed Victim-13 and provided him/her with a "Deposit Credit Statement," which falsely depicted an "opening balance" of $232,000. The "Deposit Credit Statement" was identical in format to those provided to other Victims of the CD Fraud Scheme.

70. To date, Victim-13 has not received a CD or any other investment product related to the transfer of funds described above.

3. *Victim-14*

71. In or around February 2020, Victim-14 conducted an internet search for "Best CD Rates" and discovered the Fraud Website "www.synovuswealth.com," which purported to offer the financial services of a fictitious entity called "Synovus Wealth Group" – the same Fraud Website visited by Victim-13. Victim-14 also communicated with the R.W. Fraud Contact who again used R.W.'s name and CRD number.

72. On or about February 25, 2020, Victim-14, acting on instructions provided by the R.W. Fraud Contact, sent three wires totaling approximately $931,000 to the AGQ Bank Account for what Victim-14 believed was the purchase of a CD.

73. On or about February 28, 2020, Victim-14 called the 0968 Number twice, with the calls lasting approximately 4 minutes, 52 seconds and 1 minute, 31 seconds, respectively. The length of this phone call suggests that Victim-14 and the R.W. Fraud Contact spoke about the CD that Victim-14 believed he/she had purchased and that Victim-14's calls did not simply go to voicemail.

4. *Additional Information*

74. On or about May 13, 2020 and May 14, 2020, the 0968 Number received several phone calls from 310-597-4410, the phone number listed on the Fraud Websites "www.wealthmanagementhsbc.com," and "www.globaladvisorshsbc.com."

IV. GILTMAN Controlled the AT&T Prepaid Phones

75. According to AT&T GPS and cell tower records, as well as other information gathered throughout this investigation, there is probable cause to believe that the AT&T Prepaid Phones were and are being controlled by GILTMAN. A review of AT&T records revealed that a cell phone ending in 6664, which subsequent investigation determined was subscribed to by GILTMAN at the Irvine Address (the "GILTMAN Cell Phone"), connected to many of the same AT&T cell towers at or around the same times as the AT&T Prepaid Phones, and often within minutes of each other. For example:

Tower	Date(s)	AT&T Prepaid Phone	Prepaid Phone Connect Time	Giltman Cell Phone Connect Time
Tower SADDLEBACK COLLEGE-B-55522-38522 (33.55, -117.67)	11/30/2018	3703	11/30/2018 11:36:27 am PDT	11/30/2018 11:46:55 am PDT
Tower FTLA-FSL04696_7C_1-313100175282193 (26.07, -80.15)	10/31/2019	1728	10/31/2019 5:46:35 pm EST	10/31/2019 5:36:17 pm EST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	7/15/2019	1728	7/15/2019 10:32:43 am PST	7/15/2019 10:39:29 am PST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	8/14/2019	1728	8/14/2019 2:38:36 pm PST	8/14/2019 2:30:17 pm PST

Tower	Date(s)	AT&T Prepaid Phone	Prepaid Phone Connect Time	Giltman Cell Phone Connect Time
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	10/1/2019	1728	10/1/2019 9:23:30 am PST	10/1/2019 9:50:06 am PST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	10/22/2019	1728	10/22/2019 12:43:48 pm PST	10/22/2019 12:45:03 pm PST
Tower ENCINO WEST-CLL21952_7B_1-313100143108624 (34.16, -118.52)	11/9/2019	1728	11/09/2019 9:27:04 pm PDT	11/09/2019 8:59:41 pm PDT
Tower SAND CANYON / BARRANCA-CLL03677_9B_1-310410141741321 (33.66, -117.77)	4/15/2020	0968	4/15/2020 12:30:09 pm PST	4/15/2020 12:45:14 pm PST
Tower ST PAULS GREEK ORTHODOX-CLL03138_9A_1-313100141603336 (33.67, -117.80)	2/28/2020	0968	2/28/2020 7:47:31 am PDT	2/28/2020 6:55:52 am PDT
Tower LA0496 - LAX TEMP SITE #3-A-310410141410824 (33.94, -118.40)	7/10/2019	2574	7/10/2019 2:15:41 pm PST	7/10/2019 2:19:16 pm PST
Tower JFK AIRPORT-B-310410028395901 (40.64, -73.79)	6/25/2019	2574	6/25/2019 1:31:35 pm EST	6/25/2019 2:55:55 pm EST
Tower SALT LAKE AIRPORT (GADDIS)-C-45991-10576 (40.79, -111.95)	12/19/2017	6712	12/19/2017 4:40:37 pm MDT	12/19/2017 3:54:06 pm MDT
Tower CCCO-B-27076-09822 (26.32, -80.10)	8/13/2017	6712	8/13/2017 9:50:45 am EST	8/13/2017 9:26:35 am EST
Tower SADDLEBACK COLLEGE-C-55522-38523 (33.55, -117.67)	1/19/2018	6712	1/19/2018 1:50:20 pm PDT	1/19/2018 1:14:31 pm PDT

76. An analysis of GPS and cell tower location data associated with the GILTMAN Cell Phone further revealed that the GILTMAN Cell Phone was in the same location as the AT&T Prepaid Phones at times when the AT&T Prepaid Phones made and received calls from victims of the CD Fraud Scheme. For example, as alleged above:

a. On or about December 19, 2017, at the time Victim-1 placed a call to the 6712 Number, the AT&T Prepaid Phone associated with the 6712 Number and the GILTMAN Cell Phone were in nearly the exact same location in Salt Lake City, Utah. As referenced below, travel records also show that GILTMAN was in Utah on December 19, 2017

b. On or about July 11, 2019, Victim-6 called the 2574 Number and spoke with a Fraud Contact regarding his/her CD for approximately five minutes. GPS data revealed that at approximately the same time the Victim-6 call was made, the AT&T Prepaid Phone associated with the 2574 Number and the GILTMAN Cell Phone were at the same location in Irvine, California.

77. An analysis of the location of the AT&T Prepaid Phones and the GILTMAN Cell Phone at the time of victim calls to the AT&T Prepaid Phones is reflected below:

Victim(s)	AT&T Prepaid Phone(s)	Date/Time of Victim Call(s)	Date/Time of AT&T Prepaid Phone Location	Date/Time of Giltman Cell Phone Location	Long/Lat of AT&T Prepaid Phone	Long/Lat of Giltman Cell Phone
Victim-1	6712	12/19/2017 19:40	12/19/2017 23:40	12/19/2017 23:35	-111.95016, 40.78729 Salt Lake City Airport, Salt Lake City, Utah	-111.980825, 40.785128 Salt Lake City Airport, Salt Lake City, Utah
		12/19/2017 21:49	12/19/2017 23:40	12/19/2017 23:35		
Victims-2/-3	6712	1/19/2018 14:30	1/19/2018 15:27	1/19/2018 15:27	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-4	3703	11/30/2018 18:27	11/30/2018 18:27	11/30/2018 18:31	-117.9195642, 33.6578393 Costa Mesa, California	-117.9195642, 33.6578393 Costa Mesa, California
Victim-5	3703	2/1/2019 23:32	2/1/2019 23:32	2/1/2019 23:29	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-7	2574	7/11/2019 18:22	7/11/2019 19:02	7/11/2019 18:46	-117.742134, 33.642847 Irvine, California	-117.742134, 33.642847 Irvine, California
Victims-8/-9	2574	7/11/2019 15:41	7/11/2019 15:08	7/11/2019 15:25	-117.72381, 33.637049 Irvine Industrial Complex, Irvine, California	-117.72401, 33.63734 Irvine Industrial Complex, Irvine, California
	1728	7/18/2019 17:49	7/18/2019 17:49	7/18/2019 0:00	-117.742134, 33.642847 Irvine, California	-117.742134, 33.642847 Irvine, California
Victim-10	1728	8/8/2019 20:51	8/8/2019 16:34	8/8/2019 16:38	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-12	0968	6/18/2020 18:08	6/18/2020 18:45	6/18/2020 16:17	-117.75123888889, 33.62751 Harvard Ave. & Alton Parkway Irvine, California	-117.72381, 33.637049 Harvard Ave. & Alton Parkway Irvine, California
		5/19/2020 21:39	5/19/2020 19:08	5/19/2020 19:02	-117.893395, 33.692276 South Coast Plaza Shopping Center, Coasta Mesa, California	-117.893395, 33.692276 South Coast Plaza Shopping Center, Coasta Mesa, California
Victim-13	0968	2/21/2020 16:30	2/21/2020 16:30	2/21/2020 16:34	-117.742134, 33.642847 Irvine, California	-117.742091, 33.642843 Irvine, California
Victim-14	0968	2/28/2020 16:26	2/28/2020 16:26	2/28/2020 16:28	-117.780992, 33.676881 Irvine Valley College, Irvine, California	-117.780992, 33.676881 Irvine Valley College, Irvine, California

78. Travel and financial records also confirm that GILTMAN was in control of the AT&T Prepaid Phones and used them in furtherance of the CD Fraud Scheme, including on discrete occasions in locations geographically remote from the Irvine, California area where records indicate the AT&T Prepaid Phones were typically located. For example:

a. *June 25, 2019*

i. On or about June 25, 2019, the 2574 Number connected to a cell tower located at JFK Airport in Queens, New York (the "JFK Tower") at approximately 1:31:35 EDT. According to toll records, at this time, the 2574 Number received a call from Individiual-1, a near-victim of the CD Fraud Scheme. According to Individual-1, he/she had discovered one of the Fraud Websites and was interested in purchasing a CD. On or about June 25, 2019, Individual-1 spoke with the P.S. Fraud Contact, who provided Individual-1 with information about purchasing a CD. Individual-1 became suspicious and decided not to purchase a CD through the Fraud Website.

ii. Approximately one hour later, the GILTMAN Cell Phone also connected to the JFK Tower.

iii. On or about June 15, 2019, GILTMAN purchased a plane ticket for a flight from JFK Airport to San Diego, California with a departure date of June 25, 2019.

b. *October 31, 2019*

i. On or about October 31, 2019, the 1728 Number connected to a cell tower located at Los Angeles International ("LAX") Airport in Los Angeles, California (the "LAX Tower") at approximately 8:43:32 a.m. PDT.

ii. A Capital One credit card belonging to GILTMAN was used at the LAX Airport on October 31, 2019 at 9:17:31 a.m. PDT, approximately thirty minutes after the 1728 Number connected to the LAX Tower.

iii. On or about October 31, 2019, the 1728 Number connected to a cell tower located at the Fort Lauderdale Airport in Fort Lauderdale, Florida (the "FTLA Tower") at approximately 5:46:35 p.m. EDT. Approximately ten minutes earlier, at 5:36:17 p.m. EDT, the GILTMAN Cell Phone also connected to the FTLA Tower.

iv. According to flight records, GILTMAN boarded a flight

from LAX to Fort Lauderdale on October 31, 2019. The flight left LAX at approximately 10:00 a.m. PDT, consistent with the connections described above. GILTMAN paid for the flight using an American Express card issued in his name.

c. *December 19, 2017*

i. On or about December 19, 2017, the 6712 Number connected to a cell tower located at the Salt Lake City International Airport ("SLC") in Salt Lake City, Utah (the "SLC Tower") at approximately 4:40:37 p.m. MST. Less than one hour earlier, at 3:54:06 p.m. MST, the GILTMAN Cell Phone also connected to the SLC Tower.

ii. As referenced previously, on or about December 19, 2017, at the time Victim-1 placed a call to the 6712 Number, the AT&T Prepaid Phone associated with the 6712 Number and the GILTMAN Cell Phone were in nearly the exact same location in Salt Lake City, Utah.

iii. GILTMAN boarded a flight from the Salt Lake City Airport to John Wayne Airport ("JWA") in Santa Ana, California on December 19, 2017. GPS data revealed that the 6712 Number connected to a tower located at JWA at approximately 5:30:17 p.m. PST on December 19, 2017, consistent with GILTMAN's traveling from SLC to JWA. JWA is located approximately 8 miles from the Irvine Address.

d. *August 3, 2017 – August 13, 2017*

i. On or about August 3, 2017, GILTMAN boarded a flight from LAX to Fort Lauderdale, Florida. According to flight records, GILTMAN traveled with several family members.

ii. On or about August 6, 2017, the AT&T Prepaid Phone associated with the 6712 Number was purchased and registered at a location in New York.

iii. On or about August 7, 2017, GILTMAN traveled from an airport in Fort Lauderdale, Florida to LaGuardia Airport ("LGA") in Queens, New York. The flight left Fort Lauderdale at approximately 7:07 a.m. EDT. According to airline records, GILTMAN boarded a return flight to Fort Lauderdale from LGA at approximately 8:29 p.m. EDT on the same day.

iv. On or about August 8, 2017, the AT&T Prepaid Phone associated with the 6712 Number connected to a cell tower in Boca Raton, Florida at approximately 12:36 p.m. EDT.

v. Based on this information, law enforcement believes that GILTMAN traveled to New York on August 7, 2017 to pick up the AT&T Prepaid Phone associated with the 6712 Number and then returned to Florida.

vi. On or about August 13, 2017, an American Express prepaid card (the "AMEX Prepaid Card") was purchased at a Walgreens store in Deerfield Beach, Florida (the "Deerfield Beach Walgreens") at approximately 9:34 a.m. EDT. Based on records obtained during the investigation, the AMEX Prepaid Card was thereafter used to pay for internet hosting and telecommunications services used by the Subjects in furtherance of the CD Fraud Scheme.

vii. On the same date, the 6712 Number and the GILTMAN Cell Phone connected to a cell tower in Deerfield Beach, Florida ("Tower-1") at approximately the same time that the AMEX Prepaid Card was purchased. Tower-1 is located approximately .7 miles from the Deerfield Beach Walgreens.

79. An analysis of GPS and cell tower location data associated with the GILTMAN Cell Phone further revealed that the GILTMAN Cell Phone was often at or near the same locations where and when prepaid cell phones, including the AT&T prepaid Phones, and gift cards used in furtherance of the scheme were purchased. For example:

a. On or about July 9, 2019, the prepaid phone associated with the 1728 Number was purchased at a Best Buy store at approximately 11:21 a.m. PDT. GPS records revealed that the phone associated with the 1728 Number connected to an AT&T cell tower ("Tower-2") in the vicinity of a Best Buy store in Costa Mesa, California (the "Costa Mesa Best Buy") from 11:22 a.m. PDT to 11:48 a.m. PDT. GPS records further show that the device associated with the 2574 Number, the phone used by Giltman just prior to obtaining the 1728 Number, connected to Tower-2 at approximately 11:48 a.m. PDT. The GILTMAN Cell Phone connected to the Tower-2 at approximately 11:51 a.m. PDT. Based on this information, it is believed that GILTMAN traveled to the Costa Mesa Best Buy with the device associated with the 2574 Number in order to purchase the device associated with 1728 Number in furtherance of the CD Fraud Scheme.

b. On or about September 4, 2019, an American Express prepaid gift card was purchased at a grocery store in Irvine, California (the "Irvine Grocery Store") at approximately 12:35 p.m. PDT. The gift card was subsequently used by the Subjects to pay for services related to the CD Fraud Scheme. According to GPS records, the GILTMAN Cell Phone connected to an AT&T cell tower in the vicinity of the Irvine Grocery Store ("Tower-3") at approximately 12:30 p.m. PDT. The American Express prepaid card was later used to pay for

telecommunications services used by the Subjects in furtherance of the scheme.

c. On or about October 1, 2019, three American Express prepaid gift cards were purchased at the Irvine Grocery Store at approximately 10:45 a.m. PDT. According to GPS records, the prepaid phone associated with the 1728 Number connected to Tower-3 at approximately 9:29 a.m. PDT. The GILTMAN Cell Phone connected to Tower-3 at 9:50 a.m. PDT. The American Express gift cards were subsequently used by the Subjects to pay for telecommunications and other services related to the CD Fraud Scheme.

d. On or about April 1, 2020, an American Express gift card was purchased at a CVS in Irvine, California (the "Irvine CVS") at approximately 4:04 p.m. PDT. According to GPS records, the GILTMAN Cell Phone connected to an AT&T cell tower in the vicinity of the Irvine CVS from approximately 4:01 p.m. PDT to 4:14 p.m. PDT. The American Express gift card was subsequently used by the Subjects to pay for services used in furtherance of the CD Fraud Scheme.

V. The Irelle Bank Account

80. According to records obtained during the investigation, GILTMAN is the signatory to an account at Wells Fargo Bank under the business name "Irelle Financial Corporation" (the "Irelle Bank Account"). Bank records revealed that the Irelle Bank Account was opened on or about January 21, 2012. The phone number listed for the account is the GILTMAN Cell Phone and the address listed is the Irvine Address. According to account application documents, Irelle Financial Corporation purports to be involved in the industry of "Wholesale Trade – Antique Import."

81. Irelle Financial Corporation was incorporated in California in or around 2005. GILTMAN is listed as a registered agent for the corporation.

82. An analysis of the Irelle Bank Account revealed that the account was funded primarily through international wire transfers, including at least approximately $3.5 million in international wire transfers during the relevant time period referenced in this Complaint and approximately $7.5 million since the account was opened. The wire transfers were received from numerous countries overseas, several of which were countries where victims of the CD Fraud Scheme were directed to send funds for the purchase of CDs, including, but not limited to, Hong Kong, Hungary, Turkey, and Cyprus. The entities listed on the wire transfers each had international mailing addresses, several of which were in other countries linked to the CD Fraud Scheme including Russia, Singapore, and Slovakia.

83. Many of the wire transfers into the Irelle Bank Account referenced activity that did not appear related to Irelle's stated industry of "Antique Sales,"

including numerous wire transfers that referenced "for equipment," "equipment sales," and "referral fee for coal." The investigation revealed that the Subjects and others acting on their behalf often provided financial institutions with falsified invoices to account for large wire transfers sent from victims of the CD Fraud Scheme. Many of the falsified invoices similarly referenced the sale of various industrial equipment or "equipment sales" generally.

84. A review of the Irelle Bank Account further revealed that the majority of funds received into the Irelle Bank Account were (a) transferred to a personal bank account held by GILTMAN and his wife (the "GILTMAN Bank Account"); or (b) used to make payments to American Express for a credit card belonging to GILTMAN and his immediate family. In addition to paying for everyday household living expenses, the funds were used fund a lavish lifestyle for GILTMAN, his immediate family, and extended family, which included the purchase of multiple luxury vehicles, rent for a home in a gated community, multiple domestic and international vacations including multiple Chalet rentals in the Swiss Alps and domestic winter destinations, including Deer Valley, Jackson Hole, and Aspen, private school tuition payments and education savings plans, a significant down payment for a multi-million dollar home, investment accounts (both domestic and international), and purchases made at luxury jewelers and couture retail establishments. These payments and purchases were made despite GILTMAN's apparent lack of a source of legitimate income.

85. Based on the above, law enforcement believes that the Irelle Bank Account is being used by GILTMAN to receive funds related to the CD Fraud Scheme after funds are initially wired overseas.

EXHIBIT B

Raquel R. Rivera, Esq.
William J. Hughes, Jr., Esq.
PORZIO, BROMBERG & NEWMAN, P.C.
100 Southgate Parkway
Morristown, NJ 07962-1997
(973) 538-4006
rrrivera@pbnlaw.com
wjhughes@pbnlaw.com
Attorneys for Plaintiffs
Atul H. Bhatt and Parul A. Bhatt

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ATUL H. BHATT and PARUL A. BHATT, Plaintiffs v. ALLEN GILTMAN, NOTRE GROUP LIMITED, JOHN DOES 1-10, Defendants.	**COMPLAINT** JURY TRIAL DEMANDED CIVIL ACTION NO. _____

ATUL H. BHATT and PARUL A. BHATT ("Plaintiffs") by and though their attorneys, Porzio, Bromberg & Newman, P.C., by way of Complaint, allege as follows:

NATURE OF THE COMPLAINT

1. This is a civil action stemming from a computer and wire fraud scheme perpetrated by Allen Giltman ("Giltman") together with Notre Group Limited and other unidentified individuals (John Does 1-10) (collectively "Defendants"), wherein Defendants conspired to create fraudulent websites to solicit funds on the internet from individuals seeking to invest money. Plaintiffs Atul H. Bhatt ("Mr. Bhatt") and Parul A. Bhatt ("Mrs. Bhatt") were victims of this criminal enterprise.

JURISDICTION AND VENUE

2. This court has jurisdiction over this matter pursuant to 28 U.S.C. § 1332 because the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and is between citizens of different States.

3. Venue in this Court is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred within the District of New Jersey. Specifically, Giltman, utilizing a false identity as described herein, contacted Mr. Bhatt, who he knew to be a New Jersey resident, numerous times and knowingly made false statements to Mr. Bhatt, which caused Mr. Bhatt to wire funds to him from New Jersey. The fraud, theft, and breach of contract were perpetrated in New Jersey.

PARTIES

4. Plaintiffs are residents of the State of New Jersey with a place of residence in Galloway, New Jersey.

5. Giltman is a resident of the State of California with a place of residence in Irvine, California. Giltman stole the identity of a legitimate registered investment adviser named Michael L. Hsu ("Mr. Hsu") to further his criminal enterprise.

6. Notre Group Limited is a private company located in Hong Kong.

7. John Does 1-10 conspired in a computer and wire fraud scheme whereby they created fraudulent websites to solicit funds on the internet from unsuspecting individuals, such as Plaintiffs.

8. Giltman, Notre Group Limited, and John Does 1-10 conspired together to defraud Plaintiffs.

FACTS

9. In or about September 2020, Plaintiffs endeavored to purchase a Certificate of Deposit ("CD") with approximately twenty years of their savings. Mr. Bhatt discovered a website purporting to be Asian Pacific National Bank, an Oversea-Chinese Banking Corporation ("OCBC Bank") Company, which was advertising CDs with attractive interest rates. Upon information and belief, this website was not affiliated with Asian Pacific National Bank and was engineered by Giltman, Notre Group Limited, and John Does 1-10 as part of their criminal enterprise.

10. Mr. Bhatt began corresponding via e-mail with an individual from the website who introduced himself as Mr. Hsu and utilized the e-mail address mhsubanking@protonmail.com and the phone number (951) 292-4608. Mr. Hsu held himself out to be a Senior Account Executive for Private Accounts at Asian Pacific National Bank both verbally and in writing.

11. Mr. Bhatt corresponded with Mr. Hsu for approximately one week before he and Mrs. Bhatt decided to purchase a $200,000.00 five-year CD.

12. On or about September 25, 2020, Mr. and Mrs. Bhatt filled out an application which included the insignia for Asian Pacific National Bank and was provided to them by Mr. Hsu to open the CD account. *See* Application, attached hereto as Exhibit A.

13. On or about September 25, 2020, Mr. Bhatt received an e-mail from Mr. Hsu confirming that his new account, a "60 Month Jumbo CD with Asia Pacific National Bank," was active and ready for funding. *See* Welcome E-mail, attached hereto as Exhibit B. In the e-mail, Mr. Hsu provided Mr. Bhatt an account contract number and stated that he would be the primary point of contact for any questions, comments, or feedback. Mr. Hsu also attached instructions directing Plaintiffs to wire the $200,000.00 to Asian Pacific National Bank's clearing platform, "Notre Group Limited through OCBC Bank." *See* Bank Wire Instructions, attached hereto as

Exhibit C. The wire instructions included the insignia for Asian Pacific National Bank.

14. Later that same day, Mr. Bhatt received a second e-mail from Mr. Hsu following up on whether Mr. Bhatt had completed his funding transfer and could provide a wire confirmation. *See* Wire Confirmation E-mail, attached hereto as Exhibit D. In Mr. Hsu's signature, he included CRD[1] and FDIC[2] numbers, which correspond to a registered investment adviser named Michael L. Hsu and Asian Pacific National Bank, respectively.

15. On or about September 26, 2020, Mr. Bhatt responded to Mr. Hsu's e-mails, confirming his intention to transfer the monies on September 28, 2020 and posing several follow-up questions regarding the logistics of the CD. *See* Follow-up Questions E-mail, attached hereto as Exhibit E. That same day, Mr. Hsu answered Mr. Bhatt's follow-up questions. Mr. Hsu discussed how he would be Mr. Bhatt's "personal Account Executive," explained the mechanism by which Mr. Bhatt would receive monthly interest payments, and provided an estimated value of the CD in five years if Mr. Bhatt allowed the interest to compound. *Id.*

16. On September 28, 2020, Mr. Bhatt initiated an international transfer of $200,000.00 to Notre Group Limited in Hong Kong as consideration for the 60 Month Jumbo CD with Asia Pacific National Bank promised to him by Mr. Hsu. *See* PNC Bank Receipt, attached as Exhibit F.

17. On September 29, 2020, Mr. Hsu provided Mr. Bhatt with an Initial Deposit Credit Statement, which included the insignia for Asian Pacific National Bank.. *See* Asian Pacific Bank Statement, attached as Exhibit G. Mr. Hsu also represented to Mr. Bhatt that he would be sending

[1] CRD stands for Central Registration Depository, which is a database that holds information about brokers and brokerage firms. Every stockbroker licensed to sell securities in the U.S. has a CRD number.

[2] FDIC stands for Federal Deposit Insurance Corporation. The FDIC Certificate ID is a unique number assigned to each depository institution to identify and track a bank.

him a physical CD and temporary password to log into the client portal to view his information online. *See* E-mail Chain Regarding Online Account Access, attached as Exhibit H.

18. On October 16, 2020, Mr. Bhatt contacted Mr. Hsu regarding viewing his account online. *See* Exhibit H. On October 19, 2020, Mr. Hsu reiterated that a temporary password would be sent to Mr. Bhatt shortly, but that "it has been taking a little longer than usual because of the current situation we are in now," referring to the Coronavirus Pandemic. *See* Exhibit H.

19. After Mr. and Mrs. Bhatt did not receive online access or confirming documentation regarding the CD, they contacted Asian Pacific National Bank directly. Bank personnel confirmed that Mr. and Mrs. Bhatt did not have a CD account with Asian Pacific National Bank and advised them that the man they described had been defrauding people for the last year and was under investigation by the Federal Bureau of Investigation.

20. Mr. and Mrs. Bhatt contacted both the Federal Bureau of Investigation and the Galloway Police Department to report the fraud.

21. On or about October 27, 2020, Giltman was arrested by the Federal Bureau of Investigation and charged by the U.S. Department of Justice in a four-count complaint with aggravated identity theft, conspiracy to commit wire fraud, and conspiracy to commit securities fraud, in violation of 18 U.S.C. §§ 371, 1349, 1029A(a)(1)(a) and 2. *See* Unsealed Federal Criminal Complaint against Allen Giltman, attached as Exhibit I.

22. The facts upon which Giltman was charged with stealing from fourteen identified victims, as alleged by the U.S. Department of Justice, are nearly identical to the manner upon which Giltman and his co-conspirators obtained nearly all of the Plaintiffs' life savings. That is, Giltman was alleged to assume a false identity online, falsely represent himself as a representative of a financial institution that could issue a CD, and take other victims' money before disappearing.

23. Upon information and belief, the individual purporting to be Mr. Hsu was identified by law enforcement as Giltman.

24. Upon information and belief, Giltman and others currently unknown and identified herein as John Does 1-10, conspired and worked in conjunction with each other to defraud Plaintiffs and to engage in a series of financial transactions to disguise and otherwise hide the fruits of their crimes, that is, the money that Giltman and others stole from Plaintiffs and others.

COUNT I
Common Law Fraud
(Against all Defendants)

25. Plaintiffs hereby incorporate all of the preceding allegations and make them a part of this Count as if fully set forth herein.

26. Giltman and John Does 1-10 perpetrated a fraud against Plaintiffs by holding himself out to be Mr. Hsu, a legitimate registered investment adviser, and offering to purchase a five-year CD at Asian Pacific National Bank valued at $200,000.00 on their behalf.

27. Giltman, in fact, was not Mr. Hsu and was not affiliated with Asian Pacific National Bank.

28. Giltman never intended to utilize Plaintiffs' monies to purchase a CD on their behalf.

29. Giltman made these false representations with the intent that the Plaintiffs would rely upon them and send Giltman their money, representing nearly all of their life savings.

30. Plaintiffs reasonably relied on Giltman's representation regarding his identity as well as his promise to purchase the CD and sent him $200,000.00.

31. Giltman took possession of the $200,000.00 and never purchased the CD on Plaintiffs' behalf.

32. As a result of the fraud, Plaintiffs suffered mental anguish, emotional distress, embarrassment, humiliation, financial and other losses, for which Defendants should be held jointly and severally liable, in an amount to be deemed appropriate by a jury.

COUNT II
Theft
(Against all Defendants)

33. Plaintiffs hereby incorporate all of the preceding allegations and make them a part of this Count as if fully set forth herein.

34. Plaintiffs were deprived of their right to possess their hard-earned $200,000.00 by Giltman's misrepresentations regarding his identity and his affiliation. Instead of purchasing the agreed upon CD on Plaintiffs' behalf, he took their money for his own personal gain.

35. Upon information and belief, John Does 1-10 conspired and assisted Giltman in stealing the Plaintiffs' money and concealing its ultimate location.

36. As a result of the theft, Plaintiffs suffered mental anguish, emotional distress, embarrassment, humiliation, financial and other losses, for which Defendants should be held jointly and severally liable, in an amount to be deemed appropriate by a jury.

COUNT III
Breach of Contract
(Against Giltman)

37. Plaintiffs hereby incorporate all of the preceding allegations and make them a part of this Count as if fully set forth herein.

38. Plaintiffs had a contract with Giltman wherein he offered to purchase a five-year CD at Asian Pacific National Bank valued at $200,000.00 on their behalf in exchange for the $200,000.00 deposit from Plaintiffs. Giltman materially breached the terms of this contract by failing to procure the five-year CD from Asian Pacific National Bank on Plaintiffs'

behalf and keeping Plaintiffs' $200,000.00.

39. As a result of the breach of contract, Plaintiffs suffered mental anguish, emotional distress, embarrassment, humiliation, financial and other losses in an amount to be deemed appropriate by a jury.

COUNT IV
Civil Conspiracy
(Against all Defendants)

40. Plaintiffs hereby incorporate all of the preceding allegations and make them a part of this Count as if fully set forth herein.

41. Defendants were each members of a conspiracy of two or more persons. The object of their conspiracy was to create fraudulent websites to solicit funds on the internet from unsuspecting individuals, such as Plaintiffs.

42. The members of the conspiracy had a meeting of the minds on the object or course of action. One of the members of the conspiracy committed an unlawful, overt act to further the object or course of action.

43. As a result of the conspiracy, Plaintiffs suffered mental anguish, emotional distress, embarrassment, humiliation, financial and other losses, for which Defendants should be held jointly and severally liable, in an amount to be deemed appropriate by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs demand judgment against defendants as follows:

a) Awarding Plaintiffs compensatory damages for mental anguish, emotional distress, embarrassment, humiliation, financial and other losses in an amount to be deemed appropriate by a jury.

b) Awarding Plaintiffs punitive damages, to the extent permitted by law, sufficient not only to punish defendants for their egregious unconstitutional conduct, but also to deter them from engaging in future schemes.

c) Awarding Plaintiffs attorney's fees already incurred as a result of Defendants' unlawful conduct and any reasonable attorney's fees and costs incurred.

d) Awarding Plaintiffs pre-judgment and post-judgment interest.

e) Awarding Plaintiffs all other relief that they may be entitled to under the law and all other relief that the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

PORZIO, BROMBERG & NEWMAN, P.C.
Attorneys for Plaintiffs,
Atul and Parul Bhatt

By: *s/ Raquel R. Rivera*
Raquel R. Rivera

Date: April 29, 2021

PORZIO, BROMBERG & NEWMAN, P.C.
Attorneys for Plaintiffs,
Atul and Parul Bhatt

By: *s/ William J. Hughes, Jr.*
William J. Hughes, Jr.

Date: April 29, 2021

CERTIFICATION PURSUANT TO LOCAL RULE 11.2

I certify that Allen Giltman is currently a defendant in *United States of America v. Allen Giltman*, 20-mag-13462 (LDW), currently pending in the U.S. District Court for the District of New Jersey. I am not aware that the matter in controversy is the subject of any other action pending in any court, or of any pending arbitration or administrative proceeding.

PORZIO, BROMBERG & NEWMAN, P.C.
Attorneys for Plaintiffs,
Atul and Parul Bhatt

By: *s/ Raquel R. Rivera*
Raquel R. Rivera

Date: April 29, 2021

PORZIO, BROMBERG & NEWMAN, P.C.
Attorneys for Plaintiffs,
Atul and Parul Bhatt

By: *s/ William J. Hughes, Jr.*
William J. Hughes, Jr.

Date: April 29, 2021

EXHIBIT A

EXHIBIT A

SINGLE/ JOINT ACCOUNT APPLICATION (w/ Beneficiary)

Open a CD account

Asian Pacific National Bank

OCBC WING HANG

CD Savings Account-FDIC (please circle one)

Individual Account
Joint Account
Trust Account
Business Account
IRA Account

Certificate of Deposit (please circle one)

1 Year-NO Penalty CD
2 Year CD
3 Year CD
5 Year CD
9 Month- NO Penalty CD
15 Month CD

IMPORTANT INFORMATION ABOUT OPENING A NEW ACCOUNT AT **Asia Pacific Bank** Subsidiary of Standard OCBC Banking Group FDIC

To help the United States Government fight terrorism and money laundering, Federal law requires us to obtain, verify, and record information that identifies each person that opens an account. What this means for you: when you open an account, we will ask for your name, a street address, date of birth, and an identification number, such as a Social Security number. We may also ask to view your driver's license or other identifying documents that will assist us in identifying you. We appreciate your cooperation.

Personal Information (Primary Owner)

Name Prefix:____ First Name: Atul Middle Initial: H
Last Name: Bhatt Name Suffix:____ (Jr., Sr., III, etc.)
Social Security Number: [redacted]
Date of Birth: [redacted]
Country of Residency: USA
Country of Citizenship: USA

Email and Phone (Primary Owner)

Email: [redacted]@comcast.net
Home/Cell Phone Number: [redacted]
Work Phone Number [redacted] Extension:____

Home Address (Primary Owner) — no P.O. Boxes, please

Address [redacted]
City: Galloway State: New Jersey
ZIP Code: [redacted] Years at Current Address: 16 yrs

Previous Address If at your current address less than 5 years

Address:____
City:____
State:____ ZIP Code:____

Mailing Address If different from home address

☒ Same as home address
Address:____
City:____
State:____ ZIP Code:____

Security Question

Mother's Maiden Name: [redacted]

Personal Information (Joint Owner)

Name Prefix:____ First Name: Parul Middle Initial: A.
Last Name: Bhatt Name Suffix:____ (Jr., Sr., III, etc.)
Social Security Num [redacted]
Date of Birth: [redacted]
Country of Residency: USA
Country of Citizenship: USA

Email and Phone (Joint Owner)

Email: [redacted]@comcast.net
Home/Cell Phone Number: [redacted]
Work Phone Number: [redacted] Extension:____

Home Address (Joint Owner) — no P.O. Boxes, please

Address: [redacted]
City: Galloway State: New Jersey
ZIP Code: [redacted] Years at Current Address: 16 yrs

Previous Address If at your current address less than 5 years

Address:____
City:____
State:____ ZIP Code:____

Mailing Address If different from home address

☒ Same as home address
Address:____
City:____
State:____ ZIP Code:____

Security Question

Mother's Maiden Name: [redacted]

Please note: each account can have up to 4 beneficiaries.

Choose Type of Beneficiary: ☒ POD (Payable on death) ☐ ITF (In trust for)

• Personal Information for Beneficiary (Beneficiary #1)

First Name: [redacted] Middle Initial: [redacted] Last Name: Bhatt Name Suffix: _____ (Jr., Sr., III, etc.) Date of Birt

Home Address — no P.O. Boxes please ☒ Same as Primary Owner's Address:

Address: _____ City: _____ State: _____ ZIP Code: _____

• Personal Information for Beneficiary (Beneficiary #2)

First Name: [redacted] Middle Initial: [redacted] Last Name: Bhatt Name Suffix: _____ (Jr., Sr., III, etc.) Date of Birt

Home Address — no P.O. Boxes please ☒ Same as Primary Owner's Address:

Address: _____ City: _____ State: _____ ZIP Code: _____

• Personal Information for Beneficiary (Beneficiary #3)

First Name: _____ Middle Initial: _____ Last Name: _____ Name Suffix: _____ (Jr., Sr., III, etc.) Date of Birth: _____

Home Address — no P.O. Boxes please ☐ Same as Primary Owner's Address:

Address: _____ City: _____ State: _____ ZIP Code: _____

• Personal Information for Beneficiary (Beneficiary #4)

First Name: _____ Middle Initial: _____ Last Name: _____ Name Suffix: _____ (Jr., Sr., III, etc.) Date of Birth: _____

Home Address — no P.O. Boxes, please ☐ Same as Primary Owner's Address:

Address: _____ City: _____ State: _____ ZIP Code: _____

Your Deposit Amount: $ 2 0 0 , 0 0 0 . 0 0

We cannot accept checks, money orders, cash, third-party checks, or ACH transfers. (Funding is accepted via direct Bank wire from a US Bank)

For Interest Checking and Money Market Savings Accounts:

☐ VISA® Check Card (Money Market Savings Account)

Automatic Transfers: Automatic withdrawals can be transfered from your account to an external bank account with the same ownership title.

Please withdraw $ ☐☐☐,☐☐☐.☐☐ Please start withdrawals on ____/____/____

Check One Every: ☐ Month ☐ Year

Overdraft Service Link any Online Savings or Money Market account to your Interest Checking. Also, if you exceed your checking balance, we'll transfer money from your funded savings account. Other banks charge for this transfer. With us, this back-up plan is free. Call us at: **951 292 4608** to set up overdraft service on your accounts.

Enclosed please find my personal check to activate my account. (Please, no money orders, starter checks, or third-party checks.) I understand that my account will be governed by Bank's Deposit Agreement, which will be sent to me. I agree that if the Deposit Agreement is not acceptable to me, I will close my account and receive all of my money, in full, with no fees or service charges, along with any interest owed to me.

IRS W-9 Certification. Under penalty of perjury, I certify that:
1. The number shown in this form is my correct Social Security number.
2. I am not subject to backup withholding because (a) I am exempt from backup withholding or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding, and
3. I am a U.S. person (including a U.S. resident alien).

Certification Instructions: You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. The IRS does not require your consent to any provisions of this document other than the certification required to avoid backup withholding.

In compliance with federal law, during our account opening process, we use information from your application (for example, your name, address, date of birth, and Social Security number) to verify your identity.

Signature: A Bhatt Date: 09/25/2020

Fax or email completed application to: 888-384-2341

FOR QUESTIONS, PLEASE CONTACT US AT: 951-292-4608

Member FDIC

EXHIBIT B

EXHIBIT B

Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> 9/25/2020 12:29 PM

Welcome! Your new account is now active, and ready for funding. BHATT778956 FDIC

To [redacted]@comcast.net <[redacted]@comcast.net>

Asian Pacific National Bank-A OCBC Bank Company
FDIC Insured
High Net-Worth & Wealth Management
225 W. Hospitality Ln. San Bernardino, CA 92408

September 25, 2020

Dear Mr. Atul H. Bhatt & Mrs. Parul A. Bhatt:

Joint Account W/ Beneficiaries: $200,000 FDIC

Contract # : **BHATT778956**
($1,500,000) FDIC Insured -CDARS accounts can be insured for up to $1,500,000 each.

Account Contract Number: **BHATT778956** (Asian Pacific National Bank) FDIC & CDARS $1,500,000 POD Beneficiary, Joint or Trust Account.

Asian Pacific National Bank (60 Month), Jumbo CD (3.50% APR-3.56% APY) FDIC Insured ($250,000 per account ownership category, $500,000 Joint Account) includes $250,000 additional coverage per beneficiary on the account.

No fees.

On behalf of our entire Pacific Wealth Group & OCBC staff, I'd like to take this opportunity to welcome you as a new customer.

We are thrilled to have you with us.

Included is your new account number (Contract: **BHATT778956**) your account is now active, and ready for funding. Please use it as a reference in all future correspondence. Also included as an attachment, are the wire instructions with our Clearing Platform: **Notre Group Limited through OCBC Bank** to fund your 60 Month Jumbo CD with Asia Pacific National Bank., your APY is at **3.56%. No Fees. No Penalties.**

At Asia Pacific National Wealth Group, a division of OCBC Bank, we pride ourselves on offering our customers responsive, competent and excellent service. Our customers are the most important part of our business, and we

work tirelessly to ensure your complete satisfaction, now and for as long as you are a customer.

I'm also happy to inform you that I will be your primary point of contact at the firm, and I encourage you to contact me at any time with your questions, comments and feedback.

I can be reached during regular business hours in the following ways:

Direct Phone: 951 292 4608

Email: mhsubanking@protonmail.com

Mr. & Mrs. Bhatt (Joint FDIC account W/Beneficiaries) Thank you again for entrusting Asia Pacific Banking Group with your most important business needs. We are honored to serve you.

- Asia Pacific Bank a OCBC Banking Group Reference BHATT778956.pdf (235 KB)

EXHIBIT C

EXHIBIT C

OCBC WING HANG

Asian Pacific National Bank

Cleared by Notre Group Limited through OCBC Wing Hang Bank

BANK WIRE INSTRUCTIONS

September 25, 2020

Mr. & Mrs. Bhatt,
Please use the following wire instructions to fund your account with:

Notre Group Limited / OCBC Group Company

Bank Name: OCBC WING HANG BANK
1155 YUANSHEN ROAD, PUDONG NEW AREA,
OCBC TOWER SHANGHAI, CHINA

SWIFT: OCBCCNSHXXX

Bank Account Number: 847221200012785

Account Name/Beneficiary: Notre Group Limited
Wang Fai Industrial Building
29 Luk Hop Street, 11F
San Po Kong, Kowloon, Hong Kong

Reference & Purpose . Exactly as stated: Reference # BHATT778956

EXHIBIT D

EXHIBIT D

Asian Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> 9/25/2020 5:26 PM

Wire Confirmation

To [redacted]@comcast.net <[redacted]@comcast.net>

Asian Pacific National Bank-A OCBC Bank Company
FDIC Insured
High Net-Worth & Wealth Management
225 W. Hospitality Ln. San Bernardino, CA 92408

Hello Mr. Bhatt,

I just wanted to follow-up on your funding transfer, were you able to send the funds today? Did PNC provide a receipt for you?

Have a wonderful weekend!

Respectfully,

Michael L. Hsu | Asian Pacific National Bank
Senior Account Executive
Private Accounts
225 W. Hospitality Ln. San Bernardino, CA 92408
Office: 951 292 4608
Email: mhsubanking@protonmail.com
CRD: 5442638
FDIC: 33013

EXHIBIT E

EXHIBIT E

Asian Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> 9/26/2020 1:18 PM

Re: Welcome! Your new account is now active, and ready for funding. BHATT778956 FDIC

To ATUL BHATT <[redacted]@comcast.net>

1. When the money reaches you will the currency be based on U.S. dollar or the Yuan?
The currency is in USD always for all US customers.

2. For future questions regarding my account, do I reach out to the branch located in the U.S. or the one oversees?
All questions and contact is through the branch here, in California. That is ultimately where your account is held, and I will be your personal Account Executive.

3. For interest payments what are the options for accepting, by this I mean check, direct deposit (ACH,EBT), etc..?
All interest payments will be ACH into your account between the 1st and 5th of each month. Please include a cancelled check into which account you'd like the interest sent.

4. When the CD matures will this be based upon U.S. rates or China rates?
All rates are US rates, China has nothing to do with your account, we only clear through the main branch funds are all in US at US rates.

5. If I do not take the interest every year and let it compound what will be my final balance come the end of year 5?
Your total after 5 years including principle will be $238,247.22

6. Is the final amount based upon the U.S. inflation rate or the Yuan?
All figures are in USD.

Please make sure the wire is in USD only!

Have a pleasant weekend Mr. Bhatt.

Please let me know the answers to the following questions, so we can proceed with the next steps.

------- Original Message -------
On Saturday, September 26, 2020 8:36 AM, ATUL BHATT <[redacted]@comcast.net> wrote:

> Hello,
>
> I am looking to transfer the money come this Monday 9/28/20, however I did have a few follow up questions for you that I will list below:
>
> 1. When the money reaches you will the currency be based on U.S. dollar or the Yuan?

555 226 5671

2. For future questions regarding my account, do I reach out to the branch located in the U.S. or the one oversees?
3. For interest payments what are the options for accepting, by this I mean check, direct deposit (ACH,EBT), etc..?
4. When the CD matures will this be based upon U.S. rates or China rates?
5. If I do not take the interest every year and let it compound what will be my final balance come the end of year 5?
6. Is the final amount based upon the U.S. inflation rate or the Yuan?

Please let me know the answers to the following questions, so we can proceed with the next steps.

Thank you,

Atul Bhatt

On 09/25/2020 12:29 PM Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> wrote:

Asian Pacific National Bank-A OCBC Bank Company
FDIC Insured
High Net-Worth & Wealth Management
225 W. Hospitality Ln. San Bernardino, CA 92408

September 25, 2020

Dear Mr. Atul H. Bhatt & Mrs. Parul A. Bhatt:

Joint Account W/ Beneficiaries: $200,000 FDIC

Contract # : **BHATT778956**

($1,500,000) FDIC Insured -CDARS accounts can be insured for up to $1,500,000 each.

Account Contract Number: **BHATT778956** (Asian Pacific National Bank) FDIC & CDARS $1,500,000 POD Beneficiary, Joint or Trust Account.

Asian Pacific National Bank (60 Month), Jumbo CD (3.50% APR-3.56% APY) FDIC Insured ($250,000 per account ownership category, $500,000 Joint Account) includes $250,000 additional coverage per beneficiary on the account.

No fees.

On behalf of our entire Pacific Wealth Group & OCBC staff, I'd like to take this opportunity to welcome you as a new customer.

We are thrilled to have you with us.

Included is your new account number (Contract: **BHATT778956**) your account is now active, and ready for funding. Please use it as a reference in all future correspondence. Also included as an attachment, are the wire instructions with our Clearing Platform: **Notre Group Limited through OCBC Bank** to fund your 60 Month Jumbo CD with Asia Pacific National Bank., your APY is at **3.56%. No Fees. No Penalties.**

At Asia Pacific National Wealth Group, a division of OCBC Bank, we pride ourselves on offering our customers responsive, competent and excellent service. Our customers are the most important part of our business, and we work tirelessly to ensure your complete satisfaction, now and for as long as you are a customer.

I'm also happy to inform you that I will be your primary point of contact at the firm, and I encourage you to contact me at any time with your questions, comments and feedback.

I can be reached during regular business hours in the following ways:

Direct Phone: 951 292 4608

Email: mhsubanking@protonmail.com

Mr. & Mrs. Bhatt (Joint FDIC account W/Beneficiaries) Thank you again for entrusting Asia Pacific Banking Group with your most important business needs. We are honored to serve you.

EXHIBIT F

EXHIBIT F

PNC

PNC BANK NA.
249 FIFTH AVENUE
PITTSBURGH PA 15222

Today's Date : September 28, 2020 Time : 10:28 AM, EDT

RECEIPT

SENDER :

ATUL H BHATT
[redacted]
GALLOWAY
NJ

RECIPIENT :

NOTRE GROUP LIMITED
WANG FAI INDUSTRIAL BUILDING
29 LUK HOP STREET, 11F
SAN PO KONG,KOWLOON
HONG KONG - HK

RECIPIENT'S BANK :

OCBC WING HANG BANK CHINA LIMITED
1155 YUANSHEN ROAD
PUDONG NEW AREA
SHANGHAI
20013

Confirmation Code: 209SE2830CEJ5KNF Date Available: 10/09/2020

Transfer Amount:		$ 200,000.00
Transfer Fees:		+ $ 45.00
Total Amount You Will Pay:		**$200,045.00**
Transfer Amount:		$ 200,000.00
Other Fees:	Estimated	- $ 0.00
Total to Recipient:	**Estimated**	**$ 200,000.00** *

IMPORTANT INFORMATION :

* Recipient may receive less due to fees charged by the recipient's bank and foreign taxes.

You have a right to dispute errors in your transaction. If you think there is an error, contact us within 180 days at 1-855-226-5671, M-F 9 am - 6 pm ET or www.pnc.com. You can also contact us for a written explanation of your rights.

You can cancel for a full refund within 30 minutes of payment, unless the funds have been picked up or deposited.
For questions or complaints about PNC BANK N.A., contact:

Consumer Financial Protection Bureau
855-411-2372
855-729-2372 (TTY/TDD)
www.consumerfinance.gov

PNC

PNC BANK NA.
249 FIFTH AVENUE
PITTSBURGH PA 15222

Today's Date: September 28, 2020

NOT A RECEIPT

Transfer Amount:		$ 200,000.00
Transfer Fees:		+ $ 45.00
Total Amount You Will Pay:		**$200,045.00**

Transfer Amount:		$ 200,000.00
Other Fees:	Estimated	- $ 0.00
Total to Recipient:	**Estimated**	**$ 200,000.00** *

IMPORTANT INFORMATION :

* Recipient may receive less due to fees charged by the recipient's bank and foreign taxes.

If you provide us with an incorrect account number or an incorrect recipient institution identifier for the recipient's account or institution, you may lose the Transfer Amount.

PNC

PNC BANK NA.
249 FIFTH AVENUE
PITTSBURGH PA 15222

Today's Date: September 28, 2020

NOT A RECEIPT

Transfer Amount:		$ 200,000.00
Transfer Fees:		+ $ 45.00
Total Amount You Will Pay:		**$200,045.00**

Transfer Amount:		$ 200,000.00
Other Fees:	Estimated	- $ 0.00
Total to Recipient:	**Estimated**	**$ 200,000.00** *

IMPORTANT INFORMATION :

* Recipient may receive less due to fees charged by the recipient's bank and foreign taxes.

If you provide us with an incorrect account number or an incorrect recipient institution identifier for the recipient's account or institution, you may lose the Transfer Amount.

EXHIBIT G

EXHIBIT G

Asian Pacific Bank Statement-FDIC 60 Month CD

Mr.Atul H.Bhatt & Mrs.Parul A.Bhatt
[redacted]
Galloway, NJ [redacted]

Sept. 28, 2020-Sept. 28, 2020

Asian Pacific National Bank

Account:
BHATT778956
Branch 92408

OCBC WING HANG

Account Summary

Opening Balance	$200,000.00
Withdrawals	$0.00
Deposits	$200,045.00
Closing Balance on Sept. 28, 2020	**$200,045.00**

Scan this QR code with your Smartphone

You may need to get a QR Code® reader from your SmartPhone App Store

Contact Information

800 552 2757
Contact us by phone for questions, on this statement, and change of personal information.

General inquiries:

TTY for the hearing impaired:
1-800-728-0007 code 1205

San Bernardino Branch

Your Transaction Details

Date	Details	Withdrawals	Deposits	Balance
Sept 28, 2020	Opening Balance 3.50% APY			$200,000,00
Sept 28, 2020	Wire Credit		$45.00	
	Closing Balance			**$200,045.00**

EXHIBIT H

EXHIBIT H

Asian Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> 10/19/2020 10:00 AM

Re: Opening Deposit Credit Statement BHATT778956

To ATUL BHATT <[redacted]@comcast.net>

Asian Pacific National Bank-A OCBC Bank Company
FDIC Insured
High Net-Worth & Wealth Management
225 W. Hospitality Ln. San Bernardino, CA 92408

October 19, 2020

Hello Mr. Bhatt,

In order to log into your account, you must enter your temporary pass code which will be FedExed to you shortly. Once I have the tracking number in our system I will forward that to you, as well as help get you set-up in our "Client Only Portal" to view your CD account.

It has been taking a little longer than usual because of the current situation we are in now.
Please look for an email from me in the very near time frame with the tracking number.

Please feel free to contact me anytime during business hours.

Respectfully,

Michael L. Hsu | Asian Pacific National Bank
Senior Account Executive
Private Accounts
225 W. Hospitality Ln. San Bernardino, CA 92408
Office: 951 292 4608
Email: mhsubanking@protonmail.com
CRD: 5442638
FDIC: 33013

------- Original Message -------
On Friday, October 16, 2020 6:01 PM, ATUL BHATT <[redacted]@comcast.net> wrote:

> Hello Michael,
>
> I was wondering if there was a way for me to see my account online. I see that on the confirmation that was sent to me in the PDF file there was a account number, and when I attempted to log in it asked for a security code to be send to a phone number. Both of the

numbers listed are none that belong to me, is there any way that you could tell me the process of seeing my account information online. Please let me know as soon as you can.

Thank you,

Atul Bhatt

On 09/29/2020 9:55 AM Asian Pacific National Bank-Michael Hsu <mhsubanking@protonmail.com> wrote:

Asian Pacific National Bank -A OCBC Bank Company
FDIC Insured
High Net-Worth & Wealth Management
225 W. Hospitality Ln. San Bernardino, CA 92408

September 29, 2020

Mr. & Mrs. Bhatt,

Please find your initial Deposit Credit Statement attached.
In the near future I will forward to you your FedEx tracking number which will contain your physical CD and temporary password to log in to the "Client Portal" to view your information online.

Respectfully,

Michael L. Hsu | Asian Pacific National Bank
Senior Account Executive
Private Accounts
225 W. Hospitality Ln. San Bernardino, CA 92408
Office: 951 292 4608
Email: mhsubanking@protonmail.com
CRD: 5442638
FDIC: 33013

EXHIBIT I

EXHIBIT I

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**TO BE FILED UNDER SEAL**
	:	
v.	:	Hon. Leda Dunn Wettre
	:	
ALLEN GILTMAN	:	Mag. No. **20-13462**
	:	
	:	**CRIMINAL COMPLAINT**

I, Andrew Feiter, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Andrew Feiter

Andrew Feiter, Special Agent
Federal Bureau of Investigation

Special Agent Feiter attested
to this Complaint by telephone
pursuant to FRCP 4.1(b)(2)(A) on
October 26, 2020 in the
District of New Jersey

HONORABLE LEDA DUNN WETTRE
UNITED STATES MAGISTRATE JUDGE

Leda Dunn Wettre

Signature of Judicial Officer

ATTACHMENT A

COUNT ONE

(Conspiracy to Commit Wire Fraud)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

did knowingly and intentionally conspire with others to devise and intend to devise a scheme and artifice to defraud individuals, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Sections 1349 and 2.

COUNT TWO

(Conspiracy to Commit Securities Fraud)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

knowingly and intentionally conspired and agreed with others to, by use of the means and instrumentalities of interstate commerce, the mails, and facilities of national securities exchanges, directly and indirectly, knowingly and willfully use manipulative and deceptive devices and contrivances in contravention of Title 17, Code of Federal Regulations, Section 240.10b-5 in connection with the purchases and sales of securities, to wit, Certificates of Deposit offered through various fictitious entities, by (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, namely, persons with interests in the fictitious Certificates of Deposit, contrary to Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

In violation of Title 18, United States Code, Section 371.

COUNTS THREE AND FOUR

(Aggravated Identity Theft)

From in or around October 2017 through the present, in the District of New Jersey and elsewhere, defendant

ALLEN GILTMAN

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, described in the table below, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another actual person, each constituting a separate count of this Complaint:

Count	Approximate Date	Initials of Identity Theft Victim	Means of Identification
3	April 4, 2019	M.K.	Name CRD Number
4	July 31, 2019	P.S.	Name CRD Number

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

ATTACHMENT B

I, Andrew Feiter, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed since November 2019. I am currently assigned to the Newark, New Jersey Field Office. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

2. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a federal criminal complaint and arrest warrant, I have not included each and every fact known by the Government concerning this investigation. Except as otherwise indicated, the actions, conversations, and statements of others identified in this Affidavit – even where they appear in quotations – are reported in substance and in part. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided.

PROBABLE CAUSE

I. Overview of the CD Fraud Scheme

3. The FBI is investigating an ongoing computer and wire fraud scheme that there is probable cause to believe is being executed by Allen GILTMAN ("GILTMAN") and others (the "Subjects"). In furtherance of the scheme, the Subjects have created fraudulent websites (the "Fraud Websites") to solicit funds on the internet from individuals seeking to invest money. At times, the Fraud Websites were designed to closely resemble websites being operated by actual, well-known, and publicly reputable financial institutions. For instance, the Fraud Websites "www.bnymelloncdrates.com" and "www.bnymellonpershing.com" were created to appear as real websites that were operated by and promoting the sale of investment products by the Bank of New York, an actual, well-known, and publicly reputable financial institution. At other times, the Fraud Websites were designed to resemble legitimate-seeming financial institutions that did not, in fact, exist. For example, the Fraud Websites "www.marlowefinancial.com," and "www.marlowfinancial.com" each purported to offer the investment services of a fake company calling itself "Marlow Financial."

4. The Subjects used a variety of means to make the Fraud Websites

appear legitimate and to gain and maintain the trust of prospective investors, including by:

a. displaying the actual names and logos of real financial institutions;

b. purporting that the institutions were members of and/or regulated by the Federal Deposit Insurance Corporation ("FDIC"), Financial Industry Regulatory Authority ("FINRA"), the Securities Investor Protection Corporation ("SIPC"), or New York Stock Exchange;

c. claiming that deposits made to the institutions associated with the Fraud Websites were FDIC insured; and

d. using FINRA and/or FDIC member identification numbers issued to real financial institutions and broker-dealers.

5. The Fraud Websites advertised various types of investment opportunities, most prominently the purchase of certificates of deposit ("CDs"). The Fraud Websites advertised higher than average rates of return on the CDs, which enhanced the attractiveness of the investment opportunities to potential victims.

6. Victims of the fraud, which is described herein as the "CD Fraud Scheme," typically discovered the Fraud Websites via internet searches. In furtherance of the scheme, the Subjects purchased internet advertising, which caused advertisements for the Fraud Websites to appear in Google and Microsoft Bing search results for searches including phrases such as "best CD rates" or "highest cd rates." As a result, unsuspecting investors, when conducting such internet searches, received advertisements for the Fraud Websites on their web browsers and clicked on links that directed them to the Fraud Websites.

7. Multiple victims of the CD Fraud Scheme attempted to purchase CDs that were offered through one or more of the Fraud Websites. In many instances, the victim would contact an individual via telephone or email as directed on a Fraud Website (the "Fraud Contact"). As set forth herein, there is probable cause to believe that, in many instances, the Fraud Contact was, in fact, GILTMAN, purporting to be someone else.

8. In multiple instances involving Fraud Websites that spoofed websites maintained by actual financial institutions, the Fraud Contact impersonated an actual employee of the financial institution whose name and imagery were depicted on the Fraud Website and used the real employee's name and FINRA CRD number.[1]

[1] FINRA operates the Central Registration Depository ("CRD"), the central licensing and registration system used by the U.S. securities industry and its

9. The Fraud Contact ultimately caused the victim to receive various documents, including, but not limited to, account applications, term sheets, and wiring instructions related to the purchase of a CD. The victim completed and submitted the paperwork, followed the wiring instructions, and wired funds to the bank account specified by the Fraud Contact. The funds then were moved out of the specified bank account to various international and domestic bank accounts.

10. Law enforcement has determined that the funds transmitted by the victims in accordance with the above-described procedure were not used to procure CDs or any other advertised investment products, and none of the victims actually took ownership of the products that they intended to purchase.

11. The Subjects have gone to significant lengths to hide their true identities and to perpetuate the CD Fraud Scheme. For example, they have used: (a) virtual private networks ("VPNs") to anonymize their digital footprints, such as IP addresses; (b) prepaid gift cards to pay for domain-name registration services, state incorporation filings, internet ads, and VPN, website, and call-answering services; (c) prepaid phones or encrypted communication products to communicate with victims of the CD Fraud Scheme; and (d) fake invoices and websites to explain large money transfers in response to inquiries by banks that received large wire transfers of investor funds.

12. To date, the investigation has identified at least 70 victims of the CD Fraud Scheme, who collectively transmitted funds that they believed to be investments in the amount of at least approximately $50 million. Law enforcement has further identified at least approximately 130 Fraud Websites operated by the Subjects as part of the CD Fraud Scheme. The most recent Fraud Website identified by law enforcement as part of the CD Fraud Scheme was registered on or about October 16, 2020.

II. Individuals, Entities and Bank Accounts

13. At various times relevant to this Complaint:

a. GILTMAN was a resident of California.

b. GILTMAN was the registered agent of Irelle Financial Corporation ("Irelle"), a California company, and maintained a bank account under the name "Irelle Corporation" at Wells Fargo Bank.

c. Victims -1, -4, and -10 were residents of Texas.

d. Victims -2 and-3 were residents of Connecticut.

---

regulators, which contains the registration records of broker-dealer firms and their associated individuals (*e.g.*, brokers and investment advisors).

e. Victims -5, and -12 were residents of Florida.

f. Victims -6 and -11 were residents of New Jersey.

g. Victim-7 was a resident of Massachusetts.

h. Victims -8 and -9 were residents of Georgia.

i. Victim-13 was a resident of Illinois.

j. Victim-14 was a resident of New York.

k. Individual-1 was a resident of Pennsylvania.

l. R.H., R.P., P.S., M.K., A.F., and R.W. were broker-dealers registered with FINRA.

III. The AT&T Prepaid Phones

14. Through this investigation, law enforcement has identified several AT&T prepaid phone numbers used by the Subjects in furtherance of the CD Fraud Scheme, including numbers ending in 6712 (the "6712 Number"), 1728 (the "1728 Number"), 3703 (the "3703 Number"), 2574 (the "2574 Number"), and 0968 (the "0968 Number") (collectively, the "AT&T Prepaid Phones"). The AT&T Prepaid Phones have been used by the Subjects to, for example: (a) register Fraud Websites with web-hosting providers; (b) communicate with numbers listed on the Fraud Websites to make sure the numbers were working properly; and (c) speak with victims of the CD Fraud Scheme, as set forth in the paragraphs below.

A. *The 6712 Number*

1. *Victim-1*

15. In or around October 2017, Victim-1 conducted an internet search for CDs and discovered the Fraud Website "www.marlowefinancial.com." Victim-1 called a phone number listed on the website and spoke to a Fraud Contact, who used the name of a real broker-dealer registered with FINRA with the initials R.H. (the "R.H. Fraud Contact"). The R.H. Fraud Contact told Victim-1 that "Marlowe Financial" brokered CDs from banks such as Citibank and Bank of America.

16. On or about October 20, 2017, the R.H. Fraud Contact sent Victim-1 an introductory email, which included an application for a CD, a fictitious CD term sheet, and an example of FDIC coverage. In the introductory email, the R.H. Fraud Contact again used the name of R.H. and a CRD number belonging to R.H. without R.H.'s authorization. Victim-1 thereafter applied for three CDs totaling approximately $1 million.

17. On or about October 24, 2017, the R.H. Fraud Contact sent Victim-1 an email with wiring instructions, which directed Victim-1 to wire funds to an account at TBC Bank in Tbilisi, Georgia held by an entity called "Principal Financial Limited" (the "TBC Bank Account"). Victim-1 wired the funds as instructed. In the email, the Fraud Contact provided Victim-1 with a "direct phone" number ending in 5681 (the "5681 Number").

18. On or about October 30, 2017, the Fraud Contact sent Victim-1 an email with fictitious statements related to the CDs "purchased" by Victim-1, which falsely depicted "interest earned" on the CDs as of the date of the email.

19. In or around December 2017, Victim-1 emailed the Fraud Contact to request original documents associated with the CDs that Victim-1 believed he/she had purchased. The Fraud Contact responded that the documents would be delivered to Victim-1's home by December 18, 2019.

20. On or about December 19, 2017, after not receiving the promised documents, Victim-1 twice attempted to call the Fraud Contact. According to phone records, these phone calls connected to the 6712 Number and went to voicemail. Thereafter, Victim-1 was unable to reach the Fraud Contact and never received a CD or any other investment product related to the transfer of funds described above.

2. *Victims-2 and -3*

21. In or around January 2018, Victim-2 conducted an internet search related to CDs and discovered the Fraud Website "www.principalfinancialgroupllc.com," which offered investment services through a fictitious entity called "Principal Financial Group." Victim-2 called a number listed on the Fraud Website and spoke with an individual using the name of a real broker-dealer registered with FINRA with the initials R.P. (the "R.P. Fraud Contact"). The R.P. Fraud Contact provided Victim-2 with information about FDIC limits associated with a CD promoted on the Fraud Website.

22. Victim-2's spouse, Victim-3, thereafter exchanged several emails with the R.P. Fraud Contact regarding the purchase of an FDIC insured "84 Month Jumbo CD." On or about January 18, 2018, Victim-3 received an email from the R.P. Fraud Contact welcoming Victim-2 and-3 as customers of "Principal Financial." The R.P. Fraud Contact, claiming to be a "Sr. Account Executive" with Principal Financial Group, again used the name of R.P. without R.P.'s authorization and provided the 5681 Number as a "direct phone" number - the same number provided by the R.H. Fraud Contact to Victim-1. The email further provided a fictitious account number for the CD and wiring instructions, which directed Victims-2 and -3 to wire funds to the TBC Bank Account. Victims-2 and -3 wired funds totaling approximately $242,300, as instructed, on the same date.

23. On or about January 19, 2018, Victims-2 and -3 attempted to call the R.P. Fraud Contact regarding their CD. This phone call connected to the 6712 Number and went to voicemail. Victims-2 and -3 were unable to reach the R.P. Fraud Contact and never received a CD or any other investment product related to the transfer of funds described above.

3. *Additional Information*

24. Between January 4, 2018, and February 2, 2018, the 6712 Number called the number 1-866-570-9585 on four occasions, which, during this time period, was the phone number listed on several Fraud Websites associated with the CD Fraud Scheme, including "www.theprincipalgroupllc.com," "www.marlowfinance.com," and "www.marlowecdrates.com."

25. Further, the investigation revealed that the 6712 Number was listed as the phone number for a Google email address that referenced R.H.'s name (the "R.H. Google Email Account"), but that R.H. did not create, control, or authorize. The R.H. Google Email Account was used to register at least one Fraud Website, "www.principalbrokerage.com," and was listed as a secondary email account for the Fraud Website "www.principalfinancialgroupllc.com" – the Fraud Website visited by Victims-2 and -3.

B. *The 3703 Number*

1. *Victim-4*

26. In or around November 2018, Victim-4 discovered the Fraud Website "www.federaluniversal.com," which purported to offer the investment services of an entity called "Universal Community Federal Savings Bank." Victim-4 called a number listed on the Fraud Website and spoke with an individual using the name of a real broker-dealer registered with FINRA with the initials M.K. (the "M.K. Fraud Contact"). According to Victim-4, the M.K. Fraud Contact told Victim-4 that he was located in the "financial district of Los Angeles."

27. On or about November 9, 2018, Victim-4 received an introductory email from the M.K. Fraud Contact, which included an application for a CD. The email stated, "Universal Bank is a full service, global financial institution," and represented that its products were FDIC insured. In the introductory email, the M.K. Fraud Contact again used M.K.'s name and a CRD number belonging to M.K. without M.K.'s authorization. Victim-4 thereafter applied for three CDs totaling approximately $500,000.

28. On or about November 12, 2018, Victim-4 received an email welcoming him/her as a customer and stating that his/her account was "active" and "ready for funding." The email further provided wiring instructions, which directed Victim-4 to wire funds to a bank account in Poland (the "Poland Bank Account"). Victim-4 wired the funds as instructed.

29. According to Victim-4, after he/she wired an initial $500,000, he/she received a call from the M.K. Fraud Contact, who stated that the bank was currently offering a "special" on CDs with an attractive, lower interest rate. After speaking to the M.K. Fraud Contact, Victim-4 wired an additional $500,000 to the Poland Bank Account per the M.K. Fraud Contact's instructions. Victim-4 never received a CD or any other investment product related to the transfer of funds described herein.

30. According to phone records, Victim-4 received a phone call from the 3703 Number on or about November 30, 2018, consistent with Victim-4's statement.

2. *Victim-5*

31. In or around January 2019, Victim-5 discovered the Fraud Website "www.federaluniversal.com," the same Fraud Website visited by Victim-4, which now purported to offer the financial services of a different entity called "Broadway Financial Group." The Frau Website again listed M.K.'s name and the same email address used by the M.K. Fraud Contact when communicating with Victim-4. After being provided with a CD application via email, Victim-5 opted to purchase a CD in the amount of approximately $185,000.

32. On or about January 30, 2019, Victim-5 received an email from the M.K. Fraud Contact, who again used M.K.'s name and CRD number without M.K.'s authorization. The email stated that Victim-5's account was "active" and "ready for funding" and provided wiring instructions similar to those provided to the victims referenced previously, which directed Victim-5 to wire funds to an account he/she believed belonged to "Broadway Financial Group." Victim-5 wired the funds as instructed.

33. On or about January 31, 2019, Victim-5 received an email from the M.K. Fraud Contact acknowledging the receipt of Victim-5's funds. According to Victim-5, the email listed an incorrect amount associated with the purchase of Victim-5's CD. Victim-5 became suspicious regarding the error and traveled to his/her bank to inquire about the status of the wire he/she sent. Victim-5 was informed by bank officials that the funds he/she wired were not sent to an account held by "Broadway Financial Group" as Victim-5 believed, but were rather sent to an account held at HSBC Bank by an entity called "HRC Global, LLC" (the "HRC Bank Account"). The funds were then wired to another bank account located in Hong Kong.

34. The next day, on or about February 1, 2019, Victim-5 placed at least six calls to the Fraud Contact to discuss his/her CD. Each of these calls, including one lasting approximately 2 minutes and 13 seconds, connected to the 3703 Number. To date, Victim-5 has not received a CD or any other investment product related to the transfer of funds described above.

3. *Additional Information*

35. On or about August 24, 2018, the 3703 Number called a number for TransferWise. TransferWise is an international money transfer service that at least one victim of the CD Fraud Scheme used to transfer money on the belief that he/she was purchasing a CD.

36. On or about November 15, 2018, the 3703 Number called the phone number 1-866-740-5001, which, at the time, was the phone number listed on the Fraud Website "www.midwestbankgroup.com."

37. In or around April 2019, another victim of the CD Fraud Scheme, Victim-6, visited the Fraud Website "www.midwestbankgroup.com," and wired approximately $200,000 for the purchase of a CD that Victim-6 never received. Similar to Victims -4 and -5, Victim-6 also communicated with the M.K. Fraud Contact, including an email sent to Victim-6 on or about April 4, 2019, in which the M.K. Fraud Contact used the name and CRD number of M.K. and provided Victim-6 with an application for a CD.

C. *The 2574 Number and 1728 Number*

1. *Victim-7*

38. In or around June 2019, Victim-7 discovered the Fraud Website "www.globalbankinggroupfsa.com," which purported to offer the investment services of an entity called "Global Banking Group."

39. On or about June 26, 2019, Victim-7 received an email from a Fraud Contact who used the name and CRD Number of a real broker-dealer registered with FINRA with the initials "P.S." (the "P.S. Fraud Contact"). The P.S. Fraud Contact claimed to be a "Senior Account Executive" with "Global Banking Group." The email further claimed, similar to emails received by the previous victims, that Global Bank was a "registered FDIC Institution" that offered "securities" through various FINRA/SIPC member banks such as Citibank and JP Morgan Chase. The email included an application for a "15 Month Jumbo CD."

40. On or about June 27, 2019, after completing the application provided by the P.S. Fraud Contact, Victim-7 received an email informing him/her that his/her account was "active" and "ready for funding." The email provided an account number associated with a $500,000 CD and listed a "direct phone" number for the Fraud Contact ending in 9616 (the "9616 Number"). The email further provided wiring instructions, which directed Victim-7 to wire the funds to an account held at Citibank by an entity called "HDF Global, LLC" (the "HDF Bank Account"). Victim-7 wired the funds as instructed.

41. On or about July 11, 2019, Victim-7 called the P.S. Fraud Contact regarding his/her CD. This phone call connected to the 2574 Number and lasted for approximately five minutes and seven seconds. The length of this

phone call suggests that Victim-7 and the P.S. Fraud Contact spoke about the CD that Victim-7 believed he/she had purchased and that Victim-7's call did not simply go to voicemail. Victim-7 never received a CD or any other investment product related to the transfer of funds described herein.

2. *Victims-8 and -9*

42. In or around June 2019, married couple Victims-8 and -9 discovered the Fraud Website "www.globalbankinggroupfsa.com," the same Fraud Website visited by Victim-7, after conducting an internet search for "high CD return banks." The Fraud Website advertised the services of an entity called "Global Banking Group." Similar to Victim-7, Victims-8 and -9 also communicated by phone and email with the P.S. Fraud Contact, who also provided Victims-8 and -9 with the 9616 Number.

43. On or about June 28, 2019, Victims-8 and -9 wired approximately $750,000 to the HDF Bank Account per instructions provided by the P.S. Fraud Contact. Approximately one week later, the Fraud Contact emailed Victims-8 and -9 and provided a fictitious statement regarding the status of Victims-8 and -9's CD and interest accrued on the CD to date.

44. Victims-8 and -9 became suspicious after not receiving any additional account statements. On or about July 11, 2019, Victims-8 and -9 called the P.S. Fraud Contact to inquire about the status of their CD. According to AT&T records, the call connected to the 2574 Number and lasted approximately three minutes. According to Victims-8 and -9, the P.S. Fraud Contact advised them to "give it another week" before calling back.

45. On or about July 9, 2019 the 2574 Number called the 1728 Number – the same day that the prepaid account associated with the 1728 Number was activated. Based on information learned during this investigation, the Subjects would often use one AT&T Prepaid Phone to call another, particularly when a new AT&T Prepaid Phone was first activated. Similarly, AT&T records show that the 2574 Number and the 1728 Number frequently called, or were called by, the 9616 Number, with the majority of the calls lasting just seconds. Based on this investigation, there is probable cause to believe that the Subjects were engaging in this practice in order to "test out" the AT&T Prepaid Phones, and other phones used by the Subjects, throughout the course of the CD Fraud Scheme.

46. On or about July 18, 2019, Victims-8 and -9 attempted to call the P.S. Fraud Contact approximately ten times to inquire about the status of their CD, but the calls went to voicemail. These calls all connected to the 1728 Number and lasted for just seconds each, consistent with the calls going to voicemail. Previously, as referenced above, calls made by Victims-8 and -9 to the Fraud Contact connected to the 2574 Number. Based on this information, there is probable cause to believe that the 9616 Number provided to Victims-8 and -9 by the Fraud Contact was forwarding to the 2574 and 1728 Numbers.

47. To date, Victims-8 and -9 have not received a CD or any other investment product related to the transfer of funds described above.

3. *Victim-10*

48. In or around July 2019, Victim-10 discovered the Fraud Website "www.westernalliancegroupfsa.com" after conducting an internet search for attractive CD rates. The Fraud Website purported to offer the financial services of a fictitious entity called "Western Alliance Banking Group."

49. On or about July 31, 2019, Victim-10 received an email from the P.S. Fraud Contact, the same Fraud Contact that communicated with Victims -7, -8, and -9 through various fictitious entities. The email provided Victim-10 with an application for a CD, which Victim-10 immediately completed.

50. On the same date, Victim-10 received another email from the P.S. Fraud Contact stating that his/her account was "active" and "ready for funding." The email further claimed, similar to the emails received by the victims described above, that "Western Alliance Bank is a Registered FDIC Institution" and that it offered "securities" through various financial institutions such as JP Morgan Chase, Citibank, and BB&T Bank. The email further provided wiring instructions, which directed Victim-10 to wire funds to an account held at BB&T Bank under the business name "HDS Global" (the "HDS Global Bank Account").

51. On or about August 1, 2019, Victim-10 wired approximately $250,000 to the HDS Global Bank Account per the P.S. Fraud Contact's instructions. Victim-10 thereafter received an email that confirmed receipt of the wire transfer and provided Victim-10 with a fictitious account statement showing an "opening balance" for his/her CD.

52. Victim-10 called the 1728 Number on or about August 8, 2019 and the call went to voicemail. Victim-10 never received a CD or any other investment product related to the transfer of funds described above.

4. *Additional Information*

53. On or about July 13, 2019, the Fraud Website "westernalliancebankgroup.com" was registered. Payment contact information associated with the account that created the site listed P.S.'s name and the 1728 Number.

54. On or about July 12, 2019, July 15, 2019, July 17, 2019, and July 18, 2019, the 1728 Number called numbers, which were, at the time, listed on the Fraud Websites "www.globalbankinggroupfsa.com," "www.calbusinessbank.com," "www.calcommercebanking.com," and "www.commerceonefsa.com," respectively.

55. In or around July 2019, another victim of the CD Fraud Scheme,

Victim-11, visited the Fraud Website "www.westernalliancebankgroup.com," and wired approximately $700,000 for the purchase of a CD that Victim-11 never received. Similar to Victims -7, -8, -9, and -10, Victim-11 also communicated with the P.S. Fraud Contact, including an email sent to Victim-11 on or about July 31, 2019, in which the P.S. Fraud Contact used the name and CRD number of P.S. and provided Victim-11 with an Application for a CD.

56. On or about August 19, 2019 the Fraud Website "visionbankingroup.com" was registered. The payment contact information for the account listed P.S.'s name and the 2574 Number.

D. *The 0968 Number*

1. *Victim-12*

57. In or around May 2020, Victim-12 conducted an internet search and discovered the Fraud Website "www.globalwealthhsbc.com," which purported to offer the investment services of an entity called "Global Financial Group – HSBC Wealth Management." According to Victim-12, he/she sent an email to an address displayed on the Fraud Website to inquire about purchasing a CD.

58. On or about May 12, 2020, Victim-12 received an email from a Fraud Contact who used the name and CRD number of a real broker-dealer registered with FINRA with the initials A.F. (the "A.F. Fraud Contact"). The email included an application for a CD similar to those received by previous victims of the CD Fraud Scheme.

59. On or about May 21, 2020, after returning a completed application form to the A.F. Fraud Contact, Victim-12 received an email stating this his/her account was "active" and "ready for funding." The email included wiring instructions, which directed Victim-12 to wire funds to a bank located in China. Shortly thereafter, Victim-12 wired approximately $500,000 per the Fraud Contact's instructions.

60. After completing the above transaction, Victim-12 continued to communicate with the Fraud Contact by email and phone and subsequently wired an additional $640,000 in two separate transactions for the purchase of two additional CDs through the fictitious Global Financial Group entity.

61. On or about June 18, 2020, after wiring additional funds as referenced above, Victim-12 emailed the A.F. Fraud Contact with the subject line "Call back" and stated, "I have been trying to reach you all day." The following day, on or about June 19, 2020, the Fraud Contact responded to Victim-12's email and stated, "I would like to give you my personal direct number," and listed the 0968 Number.

62. According to AT&T records, on or about June 18, 2018, the 0968 Number called Victim-12 and dialed *67 before making the call to mask the

number. The call lasted approximately three minutes and thirty-seven seconds. Further, Victim-12 called the 0968 Number at least five times between May 15, 2020 and May 20, 2020 leading up to Victim-12's initial investment through the Fraud Website. These calls occurred prior to the Fraud Contact's providing Victim-12 with the 0968 Number. There is therefore probable cause to believe that, similar to the other AT&T Prepaid Phones discussed previously, calls from victim investors were being forwarded to the 0968 Number from other numbers provided to the victims on the Fraud Websites or by a Fraud Contact through email.

63. To date, Victim-12 has not received a CD or any other investment product related to the transfer of funds described above.

2. *Victim-13*

64. In or around February 2020, Victim-13 conducted an internet search for "highest rate CD" and discovered the Fraud Website "www.synovuswealth.com," which purported to offer the investment service of an entity called "Synovus Wealth Group." Victim-13 communicated with a Fraud Contact using the name and CRD number of a real FINRA broker-dealer with the initials "R.W." (the "R.W. Fraud Contact").

65. On or about February 21, 2020, prior to purchasing a CD, Victim-13 called the 0968 Number and the call went to voicemail.

66. On or about February 24, 2020, Victim-13 received an email from the R.W. Fraud Contact. The email provided Victim-13 with an application for a CD and contained language that was nearly identical to the language in emails sent to previous victims of the CD Fraud Scheme.

67. On or about February 25, 2020, Victim-13 emailed a completed application for a CD to the R.W. Fraud Contact. The Fraud Contact responded by email, which indicated that Victim-13's account was "active" and "ready for funding." The email also included wiring instructions, which directed Victim-13 to wire funds to a Wells Fargo Bank account held under the business name AGQ Business Group LLC (the "AGQ Bank Account").

68. On February 25, 2020, Victim-13 wired approximately $232,000 to the AGQ Bank Account as instructed.

69. On February 26, 2020, the Fraud Contact emailed Victim-13 and provided him/her with a "Deposit Credit Statement," which falsely depicted an "opening balance" of $232,000. The "Deposit Credit Statement" was identical in format to those provided to other Victims of the CD Fraud Scheme.

70. To date, Victim-13 has not received a CD or any other investment product related to the transfer of funds described above.

3. *Victim-14*

71. In or around February 2020, Victim-14 conducted an internet search for "Best CD Rates" and discovered the Fraud Website "www.synovuswealth.com," which purported to offer the financial services of a fictitious entity called "Synovus Wealth Group" – the same Fraud Website visited by Victim-13. Victim-14 also communicated with the R.W. Fraud Contact who again used R.W.'s name and CRD number.

72. On or about February 25, 2020, Victim-14, acting on instructions provided by the R.W. Fraud Contact, sent three wires totaling approximately $931,000 to the AGQ Bank Account for what Victim-14 believed was the purchase of a CD.

73. On or about February 28, 2020, Victim-14 called the 0968 Number twice, with the calls lasting approximately 4 minutes, 52 seconds and 1 minute, 31 seconds, respectively. The length of this phone call suggests that Victim-14 and the R.W. Fraud Contact spoke about the CD that Victim-14 believed he/she had purchased and that Victim-14's calls did not simply go to voicemail.

4. *Additional Information*

74. On or about May 13, 2020 and May 14, 2020, the 0968 Number received several phone calls from 310-597-4410, the phone number listed on the Fraud Websites "www.wealthmanagementhsbc.com," and "www.globaladvisorshsbc.com."

IV. GILTMAN Controlled the AT&T Prepaid Phones

75. According to AT&T GPS and cell tower records, as well as other information gathered throughout this investigation, there is probable cause to believe that the AT&T Prepaid Phones were and are being controlled by GILTMAN. A review of AT&T records revealed that a cell phone ending in 6664, which subsequent investigation determined was subscribed to by GILTMAN at the Irvine Address (the "GILTMAN Cell Phone"), connected to many of the same AT&T cell towers at or around the same times as the AT&T Prepaid Phones, and often within minutes of each other. For example:

Tower	Date(s)	AT&T Prepaid Phone	Prepaid Phone Connect Time	Giltman Cell Phone Connect Time
Tower SADDLEBACK COLLEGE-B-55522-38522 (33.55, -117.67)	11/30/2018	3703	11/30/2018 11:36:27 am PDT	11/30/2018 11:46:55 am PDT
Tower FTLA-FSL04696_7C_1-313100175282193 (26.07, -80.15)	10/31/2019	1728	10/31/2019 5:46:35 pm EST	10/31/2019 5:36:17 pm EST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	7/15/2019	1728	7/15/2019 10:32:43 am PST	7/15/2019 10:39:29 am PST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	8/14/2019	1728	8/14/2019 2:38:36 pm PST	8/14/2019 2:30:17 pm PST

Tower	Date(s)	AT&T Prepaid Phone	Prepaid Phone Connect Time	Giltman Cell Phone Connect Time
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	10/1/2019	1728	10/1/2019 9:23:30 am PST	10/1/2019 9:50:06 am PST
Tower ST PAULS GREEK ORTHODOX-A-310410141603336 (33.67, -117.80)	10/22/2019	1728	10/22/2019 12:43:48 pm PST	10/22/2019 12:45:03 pm PST
Tower ENCINO WEST-CLL21952_7B_1-313100143108624 (34.16, -118.52)	11/9/2019	1728	11/09/2019 9:27:04 pm PDT	11/09/2019 8:59:41 pm PDT
Tower SAND CANYON / BARRANCA-CLL03677_9B_1-310410141741321 (33.66, -117.77)	4/15/2020	0968	4/15/2020 12:30:09 pm PST	4/15/2020 12:45:14 pm PST
Tower ST PAULS GREEK ORTHODOX-CLL03138_9A_1-313100141603336 (33.67, -117.80)	2/28/2020	0968	2/28/2020 7:47:31 am PDT	2/28/2020 6:55:52 am PDT
Tower LA0496 - LAX TEMP SITE #3-A-310410141410824 (33.94, -118.40)	7/10/2019	2574	7/10/2019 2:15:41 pm PST	7/10/2019 2:19:16 pm PST
Tower JFK AIRPORT-B-310410028395901 (40.64, -73.79)	6/25/2019	2574	6/25/2019 1:31:35 pm EST	6/25/2019 2:55:55 pm EST
Tower SALT LAKE AIRPORT (GADDIS)-C-45991-10576 (40.79, -111.95)	12/19/2017	6712	12/19/2017 4:40:37 pm MDT	12/19/2017 3:54:06 pm MDT
Tower CCCO-B-27076-09822 (26.32, -80.10)	8/13/2017	6712	8/13/2017 9:50:45 am EST	8/13/2017 9:26:35 am EST
Tower SADDLEBACK COLLEGE-C-55522-38523 (33.55, -117.67)	1/19/2018	6712	1/19/2018 1:50:20 pm PDT	1/19/2018 1:14:31 pm PDT

76. An analysis of GPS and cell tower location data associated with the GILTMAN Cell Phone further revealed that the GILTMAN Cell Phone was in the same location as the AT&T Prepaid Phones at times when the AT&T Prepaid Phones made and received calls from victims of the CD Fraud Scheme. For example, as alleged above:

a. On or about December 19, 2017, at the time Victim-1 placed a call to the 6712 Number, the AT&T Prepaid Phone associated with the 6712 Number and the GILTMAN Cell Phone were in nearly the exact same location in Salt Lake City, Utah. As referenced below, travel records also show that GILTMAN was in Utah on December 19, 2017

b. On or about July 11, 2019, Victim-6 called the 2574 Number and spoke with a Fraud Contact regarding his/her CD for approximately five minutes. GPS data revealed that at approximately the same time the Victim-6 call was made, the AT&T Prepaid Phone associated with the 2574 Number and the GILTMAN Cell Phone were at the same location in Irvine, California.

77. An analysis of the location of the AT&T Prepaid Phones and the GILTMAN Cell Phone at the time of victim calls to the AT&T Prepaid Phones is reflected below:

Victim(s)	AT&T Prepaid Phone(s)	Date/Time of Victim Call(s)	Date/Time of AT&T Prepaid Phone Location	Date/Time of Giltman Cell Phone Location	Long/Lat of AT&T Prepaid Phone	Long/Lat of Giltman Cell Phone
Victim-1	6712	12/19/2017 19:40	12/19/2017 23:40	12/19/2017 23:35	-111.95016, 40.78729 Salt Lake City Airport, Salt Lake City, Utah	-111.980825, 40.785128 Salt Lake City Airport, Salt Lake City, Utah
		12/19/2017 21:49	12/19/2017 23:40	12/19/2017 23:35		
Victims-2/-3	6712	1/19/2018 14:30	1/19/2018 15:27	1/19/2018 15:27	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-4	3703	11/30/2018 18:27	11/30/2018 18:27	11/30/2018 18:31	-117.9195642, 33.6578393 Costa Mesa, California	-117.9195642, 33.6578393 Costa Mesa, California
Victim-5	3703	2/1/2019 23:32	2/1/2019 23:32	2/1/2019 23:29	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-7	2574	7/11/2019 18:22	7/11/2019 19:02	7/11/2019 18:46	-117.742134, 33.642847 Irvine, California	-117.742134, 33.642847 Irvine, California
Victims-8/-9	2574	7/11/2019 15:41	7/11/2019 15:08	7/11/2019 15:25	-117.72381, 33.637049 Irvine Industrial Complex, Irvine, California	-117.72401, 33.63734 Irvine Industrial Complex, Irvine, California
	1728	7/18/2019 17:49	7/18/2019 17:49	7/18/2019 0:00	-117.742134, 33.642847 Irvine, California	-117.742134, 33.642847 Irvine, California
Victim-10	1728	8/8/2019 20:51	8/8/2019 16:34	8/8/2019 16:38	-117.7597377, 33.6342 Irvine, California	-117.7597377, 33.6342 Irvine, California
Victim-12	0968	6/18/2020 18:08	6/18/2020 18:45	6/18/2020 16:17	-117.75123888889, 33.62751 Harvard Ave. & Alton Parkway Irvine, California	-117.72381, 33.637049 Harvard Ave. & Alton Parkway Irvine, California
		5/19/2020 21:39	5/19/2020 19:08	5/19/2020 19:02	-117.893395, 33.692276 South Coast Plaza Shopping Center, Coasta Mesa, California	-117.893395, 33.692276 South Coast Plaza Shopping Center, Coasta Mesa, California
Victim-13	0968	2/21/2020 16:30	2/21/2020 16:30	2/21/2020 16:34	-117.742134, 33.642847 Irvine, California	-117.742091, 33.642843 Irvine, California
Victim-14	0968	2/28/2020 16:26	2/28/2020 16:26	2/28/2020 16:28	-117.780992, 33.676881 Irvine Valley College, Irvine, California	-117.780992, 33.676881 Irvine Valley College, Irvine, California

78. Travel and financial records also confirm that GILTMAN was in control of the AT&T Prepaid Phones and used them in furtherance of the CD Fraud Scheme, including on discrete occasions in locations geographically remote from the Irvine, California area where records indicate the AT&T Prepaid Phones were typically located. For example:

a. *June 25, 2019*

i. On or about June 25, 2019, the 2574 Number connected to a cell tower located at JFK Airport in Queens, New York (the "JFK Tower") at approximately 1:31:35 EDT. According to toll records, at this time, the 2574 Number received a call from Individiual-1, a near-victim of the CD Fraud Scheme. According to Individual-1, he/she had discovered one of the Fraud Websites and was interested in purchasing a CD. On or about June 25, 2019, Individual-1 spoke with the P.S. Fraud Contact, who provided Individual-1 with information about purchasing a CD. Individual-1 became suspicious and decided not to purchase a CD through the Fraud Website.

ii. Approximately one hour later, the GILTMAN Cell Phone also connected to the JFK Tower.

iii. On or about June 15, 2019, GILTMAN purchased a plane ticket for a flight from JFK Airport to San Diego, California with a departure date of June 25, 2019.

b. *October 31, 2019*

i. On or about October 31, 2019, the 1728 Number connected to a cell tower located at Los Angeles International ("LAX") Airport in Los Angeles, California (the "LAX Tower") at approximately 8:43:32 a.m. PDT.

ii. A Capital One credit card belonging to GILTMAN was used at the LAX Airport on October 31, 2019 at 9:17:31 a.m. PDT, approximately thirty minutes after the 1728 Number connected to the LAX Tower.

iii. On or about October 31, 2019, the 1728 Number connected to a cell tower located at the Fort Lauderdale Airport in Fort Lauderdale, Florida (the "FTLA Tower") at approximately 5:46:35 p.m. EDT. Approximately ten minutes earlier, at 5:36:17 p.m. EDT, the GILTMAN Cell Phone also connected to the FTLA Tower.

iv. According to flight records, GILTMAN boarded a flight

from LAX to Fort Lauderdale on October 31, 2019. The flight left LAX at approximately 10:00 a.m. PDT, consistent with the connections described above. GILTMAN paid for the flight using an American Express card issued in his name.

c. *December 19, 2017*

i. On or about December 19, 2017, the 6712 Number connected to a cell tower located at the Salt Lake City International Airport ("SLC") in Salt Lake City, Utah (the "SLC Tower") at approximately 4:40:37 p.m. MST. Less than one hour earlier, at 3:54:06 p.m. MST, the GILTMAN Cell Phone also connected to the SLC Tower.

ii. As referenced previously, on or about December 19, 2017, at the time Victim-1 placed a call to the 6712 Number, the AT&T Prepaid Phone associated with the 6712 Number and the GILTMAN Cell Phone were in nearly the exact same location in Salt Lake City, Utah.

iii. GILTMAN boarded a flight from the Salt Lake City Airport to John Wayne Airport ("JWA") in Santa Ana, California on December 19, 2017. GPS data revealed that the 6712 Number connected to a tower located at JWA at approximately 5:30:17 p.m. PST on December 19, 2017, consistent with GILTMAN's traveling from SLC to JWA. JWA is located approximately 8 miles from the Irvine Address.

d. *August 3, 2017 – August 13, 2017*

i. On or about August 3, 2017, GILTMAN boarded a flight from LAX to Fort Lauderdale, Florida. According to flight records, GILTMAN traveled with several family members.

ii. On or about August 6, 2017, the AT&T Prepaid Phone associated with the 6712 Number was purchased and registered at a location in New York.

iii. On or about August 7, 2017, GILTMAN traveled from an airport in Fort Lauderdale, Florida to LaGuardia Airport ("LGA") in Queens, New York. The flight left Fort Lauderdale at approximately 7:07 a.m. EDT. According to airline records, GILTMAN boarded a return flight to Fort Lauderdale from LGA at approximately 8:29 p.m. EDT on the same day.

iv. On or about August 8, 2017, the AT&T Prepaid Phone associated with the 6712 Number connected to a cell tower in Boca Raton, Florida at approximately 12:36 p.m. EDT.

v. Based on this information, law enforcement believes that GILTMAN traveled to New York on August 7, 2017 to pick up the AT&T Prepaid Phone associated with the 6712 Number and then returned to Florida.

vi. On or about August 13, 2017, an American Express prepaid card (the "AMEX Prepaid Card") was purchased at a Walgreens store in Deerfield Beach, Florida (the "Deerfield Beach Walgreens") at approximately 9:34 a.m. EDT. Based on records obtained during the investigation, the AMEX Prepaid Card was thereafter used to pay for internet hosting and telecommunications services used by the Subjects in furtherance of the CD Fraud Scheme.

vii. On the same date, the 6712 Number and the GILTMAN Cell Phone connected to a cell tower in Deerfield Beach, Florida ("Tower-1") at approximately the same time that the AMEX Prepaid Card was purchased. Tower-1 is located approximately .7 miles from the Deerfield Beach Walgreens.

79. An analysis of GPS and cell tower location data associated with the GILTMAN Cell Phone further revealed that the GILTMAN Cell Phone was often at or near the same locations where and when prepaid cell phones, including the AT&T prepaid Phones, and gift cards used in furtherance of the scheme were purchased. For example:

a. On or about July 9, 2019, the prepaid phone associated with the 1728 Number was purchased at a Best Buy store at approximately 11:21 a.m. PDT. GPS records revealed that the phone associated with the 1728 Number connected to an AT&T cell tower ("Tower-2") in the vicinity of a Best Buy store in Costa Mesa, California (the "Costa Mesa Best Buy") from 11:22 a.m. PDT to 11:48 a.m. PDT. GPS records further show that the device associated with the 2574 Number, the phone used by Giltman just prior to obtaining the 1728 Number, connected to Tower-2 at approximately 11:48 a.m. PDT. The GILTMAN Cell Phone connected to the Tower-2 at approximately 11:51 a.m. PDT. Based on this information, it is believed that GILTMAN traveled to the Costa Mesa Best Buy with the device associated with the 2574 Number in order to purchase the device associated with 1728 Number in furtherance of the CD Fraud Scheme.

b. On or about September 4, 2019, an American Express prepaid gift card was purchased at a grocery store in Irvine, California (the "Irvine Grocery Store") at approximately 12:35 p.m. PDT. The gift card was subsequently used by the Subjects to pay for services related to the CD Fraud Scheme. According to GPS records, the GILTMAN Cell Phone connected to an AT&T cell tower in the vicinity of the Irvine Grocery Store ("Tower-3") at approximately 12:30 p.m. PDT. The American Express prepaid card was later used to pay for

telecommunications services used by the Subjects in furtherance of the scheme.

c. On or about October 1, 2019, three American Express prepaid gift cards were purchased at the Irvine Grocery Store at approximately 10:45 a.m. PDT. According to GPS records, the prepaid phone associated with the 1728 Number connected to Tower-3 at approximately 9:29 a.m. PDT. The GILTMAN Cell Phone connected to Tower-3 at 9:50 a.m. PDT. The American Express gift cards were subsequently used by the Subjects to pay for telecommunications and other services related to the CD Fraud Scheme.

d. On or about April 1, 2020, an American Express gift card was purchased at a CVS in Irvine, California (the "Irvine CVS") at approximately 4:04 p.m. PDT. According to GPS records, the GILTMAN Cell Phone connected to an AT&T cell tower in the vicinity of the Irvine CVS from approximately 4:01 p.m. PDT to 4:14 p.m. PDT. The American Express gift card was subsequently used by the Subjects to pay for services used in furtherance of the CD Fraud Scheme.

V. The Irelle Bank Account

80. According to records obtained during the investigation, GILTMAN is the signatory to an account at Wells Fargo Bank under the business name "Irelle Financial Corporation" (the "Irelle Bank Account"). Bank records revealed that the Irelle Bank Account was opened on or about January 21, 2012. The phone number listed for the account is the GILTMAN Cell Phone and the address listed is the Irvine Address. According to account application documents, Irelle Financial Corporation purports to be involved in the industry of "Wholesale Trade – Antique Import."

81. Irelle Financial Corporation was incorporated in California in or around 2005. GILTMAN is listed as a registered agent for the corporation.

82. An analysis of the Irelle Bank Account revealed that the account was funded primarily through international wire transfers, including at least approximately $3.5 million in international wire transfers during the relevant time period referenced in this Complaint and approximately $7.5 million since the account was opened. The wire transfers were received from numerous countries overseas, several of which were countries where victims of the CD Fraud Scheme were directed to send funds for the purchase of CDs, including, but not limited to, Hong Kong, Hungary, Turkey, and Cyprus. The entities listed on the wire transfers each had international mailing addresses, several of which were in other countries linked to the CD Fraud Scheme including Russia, Singapore, and Slovakia.

83. Many of the wire transfers into the Irelle Bank Account referenced activity that did not appear related to Irelle's stated industry of "Antique Sales,"

including numerous wire transfers that referenced "for equipment," "equipment sales," and "referral fee for coal." The investigation revealed that the Subjects and others acting on their behalf often provided financial institutions with falsified invoices to account for large wire transfers sent from victims of the CD Fraud Scheme. Many of the falsified invoices similarly referenced the sale of various industrial equipment or "equipment sales" generally.

84. A review of the Irelle Bank Account further revealed that the majority of funds received into the Irelle Bank Account were (a) transferred to a personal bank account held by GILTMAN and his wife (the "GILTMAN Bank Account"); or (b) used to make payments to American Express for a credit card belonging to GILTMAN and his immediate family. In addition to paying for everyday household living expenses, the funds were used fund a lavish lifestyle for GILTMAN, his immediate family, and extended family, which included the purchase of multiple luxury vehicles, rent for a home in a gated community, multiple domestic and international vacations including multiple Chalet rentals in the Swiss Alps and domestic winter destinations, including Deer Valley, Jackson Hole, and Aspen, private school tuition payments and education savings plans, a significant down payment for a multi-million dollar home, investment accounts (both domestic and international), and purchases made at luxury jewelers and couture retail establishments. These payments and purchases were made despite GILTMAN's apparent lack of a source of legitimate income.

85. Based on the above, law enforcement believes that the Irelle Bank Account is being used by GILTMAN to receive funds related to the CD Fraud Scheme after funds are initially wired overseas.

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Atul H. Bhatt and Parul A. Bhatt

(b) County of Residence of First Listed Plaintiff **Atlantic County, NJ**
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Raquel R. Rivera, Esq. and William J. Hughes, Jr., Esq.
Porzio, Bromberg & Newman, PC,
100 Southgate Parkway, Morristown, NJ 07960

DEFENDANTS
Allen Giltman, Notre Group Limited, and John Does 1-10
County of Residence of First Listed Defendant **Orange County, CA**
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff) (For Diversity Cases Only) and One Box for Defendant)*

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☒ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)* Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury – Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 U.S.C. 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. v/Disabilities – Employment
- ☐ 446 Amer. w/Disabilities – Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee – Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (***Do not cite jurisdictional statutes unless diversity***): **28 U.S.C. § 1332**

Brief description of cause: This is a civil action stemming from a computer and wire fraud scheme perpetrated by Allen Giltman together with Notre Group Limited and other unidentified individuals, wherein Defendants conspired to create fraudulent websites to solicit funds on the internet from individuals seeking to invest money. Plaintiffs were victims of this criminal enterprise.

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv. P.

DEMAND $200,000 plus punitive damages, interest, costs, and attorney's fees.

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):* JUDGE **Hon. Lena Dunn Wettre** DOCKET NUMBER **20-mag-13462 (LDW)**

DATE: **April 29, 2021** SIGNATURE OF ATTORNEY OF RECORD: ***s/Raquel R. Rivera***

FOR OFFICE USE ONLY
RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____